To Retaliate or Not:
A Matter of Cyber Risk Perception



Monica Kaminska

Kellogg College
University of Oxford

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Hilary Term
2021

88,662 words

For my parents, who supported me every step of the way

Table of Contents

Abstract *i*

List of Tables and Figures *ii*

Acknowledgements *iii*

1 Introduction: The Cyber Response Dilemma and the Risk Society **1**

1.1 The research puzzle and research question 1

1.2 Summary of the argument: the "risk society" meets cyber conflict 8

1.3 The risk society theory in international security studies 14

1.4 Theoretical and empirical contributions of the thesis 15

1.5 Methods and data 17

1.5.1 Case study approach 17

1.5.2 Case selection 18

1.5.3 Data collection 19

1.6 Structure of the thesis 20

2 Conceptual Framework: The Risk Society **23**

2.1 Introduction 23

2.2 Existing literature 24

2.2.1 Rational choice theories 24

A. Neorealism 25

B. Neoliberalism 28

2.2.2 Cognitive and psychological approaches 30

2.2.3 Constructivist approaches 32

2.3 The risk framework 36

2.3.1 The origins of the risk framework in Sociology 37

2.3.2 Defining risk 39

2.3.3 The threat society: a refinement of risk society thinking 41

2.3.4 Challenges to the risk society thesis 45

2.4 Conclusion 46

3 The Risk Society and Threat Society in the Cyber Domain: Reactions to Operational Uncertainty **48**

3.1 Introduction 48

3.2 Sources of operational uncertainty in the cyber domain 49

3.2.1 Operational characteristic 1: cyberspace as a "complex adaptive" system 49

3.2.2 Operational characteristic 2: ease of proliferation 51

3.3 Cyberspace and uncertainty: how operational characteristics can complicate responses 53

3.3.1 Consequence 1: the attribution problem: the risk of misattribution and plausible deniability 53

3.3.2 Consequence 2: the risk of unintended effects: collateral damage, blowback, and escalation 55

3.4 Risk management practices 58
3.4.1 Preventive action 58
3.4.2 Increasing resilience 60
3.4.3 Consequence management 61
3.5 Threat societies 62
3.6 Conclusion 63

4 The United States: A Risk Manager in a Networked World 65
4.1 Introduction 65
4.2 An overview of US cyber victimhood 67
4.3 The birth of the US risk society 74
4.4 The rejection of meaningful reprisal: the risk society (in)action 80
4.4.1 Concerns about the cyber operational environment: proliferation and complex adaptiveness 81
4.4.2 Concerns about the risk of misattribution and plausible deniability 83
4.4.3 Concerns about the risk of unintended effects (collateral damage, blowback, and escalation) 86
4.5 US risk management practices: evolution from caution to proactiveness 92
4.5.1 Increasing resilience 93
4.5.2 Consequence management 94
4.5.3 Preventive action 95
4.6 Conclusion 100

5 Israel and the Culture of Over-Punishment: The Threat Society in Action 102
5.1 Introduction 102
5.2 An overview of cyber attacks targeting Israel and its responses 104
5.3 The sources of meaningful responses: strategic culture and the threat society 108
5.3.1 The siege mentality 111
5.3.2 The problem-solving attitude 115
5.3.3 The cult of the offense 116
5.4 The influence of the threat society on Israel's deterrence strategy and responses to cyber attacks 117
5.4.1 Israel's conventional deterrence strategy 118
5.4.2 Israel's conventional deterrence strategy in the cyber domain 120
A. Focus on the attacker (threat) 121
B. Forceful punishment and acceptance of escalation risks 122
C. Intentional unpredictability and the right to a military response 123
5.4.3 Cyber conflict as another "Iran issue" 125
5.4.4 Israel's response to Iran's water system attack 128
5.5 Prevention, resilience-building, and consequence management 130
5.5.1 "Mabam": the campaign between wars 130
5.5.2 Low-end measures: resilience-building and consequence management 132
5.6 Conclusion 134

6 Estonia: A Threat Society Embedded in a Risk Community Alliance **136**
6.1 Introduction 136
6.2 The relevance of the 2007 cyber attacks to Estonia's national security 138
6.3 Estonia: a threat society within a larger risk community 143
6.3.1 Estonia as a threat society 144
6.3.2 In search of NATO: combining total defence with collective defence 146
6.3.3 Estonia: a risk pretender? 149
6.3.4 Estonia's rejection of meaningful punishment: appeasing the risk community 154
6.4 Estonia in the cyber domain after 2007: a threat society still absorbed by Russia 159
6.5 Conclusion 167

7 Conclusion: Contributions, Policy Implications, and Further Research **169**
7.1 Introduction 169
7.2 Key empirical findings 170
7.2.1 Views of the operational environment and escalation 172
7.2.2 The problem of attribution 173
7.2.3 Differences in preventive action 174
7.3 Contributions to International Relations scholarship 175
7.4 Implications for cyber studies and cybersecurity policy 177
7.5 Recent developments and general trends 180
7.6 Avenues for further research 183

Bibliography *185*

To Retaliate or Not: A Matter of Cyber Risk Perception

Monica Kaminska
Kellogg College
Hilary Term 2021
Doctor of Philosophy

Abstract

This thesis investigates variation in state responses to hostile cyber operations. The central argument is that states' strategic cultures and historical experiences shape their risk attitudes in cyber attack scenarios, with important consequences for their willingness (or not) to carry out meaningful punishment. To guide the empirical investigation, the thesis develops a conceptual framework drawing from and adapting the "risk society" theory in Sociology – an approach that has not yet been applied in cyber studies. The thesis explains weak state responses as a result of cultural and historical forces that produce sensitivities to the inherent risks and uncertainties of the operational environment of cyberspace. It explains strong state responses as the result of a different sensitivity: preoccupation with an existential threat, which produces a willingness to accept operational risks.

Conceptually, the thesis contributes to domestic-level constructivism in International Relations by elaborating upon the historical and cultural roots of national risk profiles in cyber conflict scenarios. Empirically, it applies the risk framework to three case studies. It argues that as a risk society, the United States failed to punish cyber attacks meaningfully due to concerns about risks arising from the operational environment – particularly the risk of conflict escalation. By contrast, Israel – a threat society – carried out strong punishment because of its preoccupation with the existential threat posed by Iran, which prompted Israel to tolerate operational risks. Although Estonia was also a threat society, it moderated its response to cyber attacks because of its membership within NATO, a risk community whose sensitivities Estonian officials decided to appease because of their desire to retain alliance support in face of the perceived existential threat posed by Russia.

List of Tables

Table 1: Cyber operations against the United States 4

Table 2: Cyber operations against Israel 7

Table 3: Cyber operations against Estonia 8

Table 4: The risk spectrum 42

Table 5: The interaction between the operational characteristics of cyberspace and risk society sensitivities 62

Acknowledgements

First and foremost, my deep gratitude goes to Lucas Kello for his unwavering support throughout my time at Oxford. I finished this thesis in the midst of a global pandemic and while starting a new job abroad. Without Lucas' steady intellectual guidance and kind reassurance, the completion of this project would not have been possible. I am very fortunate to have worked with such a sharp-minded and generous scholar.

I would also like to thank Christopher Coker who inspired the conceptual framework for this thesis over a lunch at the LSE in May 2018. Christopher's brilliant thinking, which I was lucky enough to have engaged with first-hand as an undergraduate, was also what motivated me to return to academia and pursue a doctorate in the first place. I only hope that I have done justice to his work here.

Many more academics and institutions helped to bring this project to fruition. I am very grateful to my Viva examiners, Richard Harknett and Joss Wright, who engaged deeply with my work and whose searching questions elevated my thinking. My examination with them instilled in me a confidence that will accompany me in my future academic pursuits. Dominic Johnson and Corneliu Bjola offered insightful advice during my Confirmation of Status at the Department of Politics and International Relations (DPIR). Andrew Martin, along with David Hobbs, Maureen York, and Katherine Fletcher, provided a welcoming and supportive environment for my research at the Centre for Doctoral Training in Cyber Security (CDT). Overall, I benefitted enormously from the diverse intellectual setting provided by DPIR, the CDT, and the Department of Computer Science. I am grateful to the Engineering and Physical Sciences Research Council for enabling my studies with their generous financial support and for funding my industrial placement at Sophos in the summer of 2019. I am thankful to Andrew Dwyer for facilitating that valuable professional experience.

This thesis could not have been completed without the support of incredible friends and colleagues in Oxford. Martin Krämer, Arianna Schuler-Scott, and Jack Sturgess were always there when I needed them. James Shires, Max Smeets, Florian Egloff, and Jamie Collier enthusiastically discussed my ideas and integrated me into the university's community of cyber scholars. Dorothy Nicholas, Jan Silomon, and Takis Metaxas made my time at Oxford memorable. Valentin Weber, Rob Gorwa, and Abhishek Dasgupta were valuable cyber-confidants. Thank you to the diverse communities of the CDT and the Cyber Studies Programme in DPIR.

Dozens of individuals beyond Oxford supported my research by generously giving their time and opening their networks to me. In particular, Gabi Siboni's dedication to helping me reach key individuals in Israel and Toomas Hendrik Ilves's enthusiasm in Estonia stand out. Thank you to each and every one of my interviewees. I was also very fortunate to have opportunities to present my research at numerous academic venues and workshops, including Columbia University's School of International and Public Affairs, the University of New South Wales, The Hague Program for Cyber Norms, and the International Studies Association.

I am indebted also to my colleagues at Leiden University where I started a postdoctoral fellowship in 2020. In particular, I am grateful to Dennis Broeders for his patience and understanding and to Bibi van den Berg, Fabio Cristiano, Corianne Oosterbaan, Tatiana Tropina, Els de Busser, and Tommy van Steen for their good humour and warm company in The Hague.

Most importantly, I would like to extend my gratitude to my family and friends. I am immensely grateful to my grandma Janina, my late uncle Paweł, Tony, and Ewa for their constant encouragement. This thesis is dedicated to my parents. Their steadfast presence and unconditional support made this all possible.

Chapter 1
Introduction: The Cyber Response Dilemma and the Risk Society

1.1 The research puzzle and research question[1]

When the United States falls victim to major foreign cyber attacks, it faces a punishment problem: despite formally adopting a strategy of deterrence,[2] it struggles to meaningfully respond to major operations whose effects are significant to national security. The unwillingness to issue meaningful responses has eroded adversaries' expectation of reprisal for such attacks, which increases the likelihood that the operations will continue to grow in number. As the Cyberspace Solarium Commission, established by US Congress to explore, among other things, the response problem, noted, "[t]oday most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure. … [T]hrough our inability or unwillingness to identify and punish our cyber adversaries, we are signalling that interfering in American elections or stealing billions in U.S. intellectual property is acceptable."[3]

In addition, US policymakers have issued public attribution statements in which they have highlighted the level of destructiveness of attacks and promised consequences.[4] Public attribution in itself should significantly raise the probability of punishment. "In cases where the victim lacks an appropriate response," wrote Jon Lindsay, "publicly blaming the perpetrator without backing it up only makes the victim look weak."[5] In other words, if a state issues an attribution statement but does not

---

[1] Parts of this chapter appear in Monica Kaminska, 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks', *Journal of Cybersecurity* 7, no. 1 (9 March 2021), https://doi.org/10.1093/cybsec/tyab008.

[2] The United States has stated it will pursue not only "deterrence by denial," or "efforts [that] aim to persuade adversaries that the United States can thwart malicious cyber activity," but crucially also "deterrence by cost imposition," or "measures [that] are designed to both threaten and carry out actions to inflict penalties and costs against adversaries that choose to conduct cyber attacks or other malicious cyber activity against the United States." See: The White House, 'National Cyber Strategy of the United States of America' (Washington, D.C.: The White House, September 2018), 21, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; White House, 'Report on Cyber Deterrence Policy', 2015, http://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf..

[3] Angus King and Mike Gallagher, eds., 'United States of America Cyberspace Solarium Commission', March 2020, v, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[4] The White House, 'Statement from the Press Secretary', 15 February 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/; Foreign and Commonwealth Office, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks', gov.uk, 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[5] Jon R. Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack', *Journal of Cybersecurity* 1, no. 1 (27 November 2015): 58, https://doi.org/10.1093/cybsec/tyv003; Benjamin Edwards et al., 'Strategic Aspects of Cyberattack, Attribution, and Blame', *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (2017): 2825, https://doi.org/10.1073/pnas.1700442114.

follow up with punishment, it incurs a reputation cost and communicates that it is either unable or unwilling to retaliate despite suffering significant losses.[6]

The United States is not alone in its cyber response dilemma. In one of the first instances of cross-border cyber conflict in 2007, Estonia also failed to issue any response to what it believed to be a series of Russian-sponsored distributed denial of service (DDoS) attacks,[7] which severely disrupted civilian life in the country for about three weeks. Importantly, Estonia did have response options. Three years prior to the attacks, the country had joined NATO, precisely to protect itself from Russian aggression. Yet, at a time of peak hostility between Russia and Estonia, which involved not just the DDoS operation but also street violence conducted by members of the country's ethnic Russian minority, the Estonian government did not seek any formal alliance proceedings against Russia.

A third state, Israel, takes a very different approach towards hostile cyber operations. In May 2019, Israel conducted a physical air strike against the offensive cyber unit of Hamas. According to media reporting, the strike against Hamas' cyber facilities was a case of "immediate physical retaliation."[8] A year later, in May 2020, after a reported Iranian breach into Israeli water distribution networks, Israel retaliated with a highly disruptive cyber attack on Iran's Shahid Rajaee port facility, the main maritime gateway into the country.[9] Like the United States and Estonia, Israel is a state enormously dependent on digital infrastructures and therefore similarly vulnerable to the potentially grave disruptions of escalating cyber conflict. Moreover, Israel is a liberal democracy, thereby sharing fundamental political values and institutions with the United States and Estonia. Israel is also similar to Estonia in that it exists in a geopolitically hostile environment. Yet, Israel responded to cyber attacks differently. Taken together, therefore, the different response attitudes of the three countries present a glaring empirical puzzle. Why did states that are liberal democracies and equally technologically advanced and dependent on cyberspace respond to cyber attacks so differently? Furthermore, why did two states facing similar external threats also behave differently?

---

[6] Lindsay, 'Tipping the Scales', 58; Edwards et al., 'Strategic Aspects of Cyberattack, Attribution, and Blame', 2829; Jack Goldsmith and Robert D. Williams, 'The Failure of the United States' Chinese-Hacking Indictment Strategy', Lawfare, 28 December 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

[7] DDoS attacks involve websites being flooded and overwhelmed with information requests, thus making them unavailable to legitimate Internet users. See: Will Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 110.

[8] Kate O'Flaherty, 'Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First', *Forbes*, 6 May 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/.

[9] Joby Warrick and Ellen Nakashima, 'Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility', *The Washington Post*, 18 May 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html; SeaNews, 'Iran Plans to Bring Its Shahid Rajaee Port to State-of-Art Status', SeaNews Turkey, 7 September 2019, https://www.seanews.com.tr/iran-plans-to-bring-its-shahid-rajaee-port-to-state-of-art-status/183880/.

In this thesis, the term "meaningful punishment" or "meaningful response" denotes the imposition of "swift, costly, and transparent consequences" to "deter future bad behavior," as stated in the US National Cyber Strategy.[10] As Lindsay noted, meaningful punishment is essential to establish that the state in question has the credible will and capability to respond to attacks in the future.[11] The imposition of meaningful punishment, however, does not necessarily entail the objective of influencing the adversary to abandon their future offensive plans altogether. As scholars have pointed out, absolute deterrence was a rare Cold War exception owing to the enormously destructive nature of nuclear weapons.[12] Rather, meaningful punishment is meant to affect an adversary such that they will restrain or otherwise modify their actions in order to moderate or avoid a future punishment.[13]

Thomas Schelling offered an additional elaboration on how to deter an adversary through meaningful punishment. He argued that the "idiom of reprisal" is only effective when there is a connection between an action and a reprisal. He therefore recommended that actions should be part of a "coherent pattern"; a response should be mounted in the same "currency" and "language" and the enemy has to be able to clearly determine that the punitive measures implemented are a form of reprisal as opposed to opportunistic assault.[14] In other words, in order for a punishment to be meaningful, it has to communicate a clear message by means of its intensity and specificity.

To showcase the contrasting responses of the United States, Estonia, and Israel, the tables below describe the most significant cyber incidents that afflicted these countries and summarise their reactions. Significant in this context means successful or attempted acts of sabotage or subversion. Sabotage is defined as "a deliberate attempt to weaken or destroy an economic or military system" (including DDoS attacks) and subversion as "a deliberate attempt to undermine the authority, integrity, and constitution of established authority and order."[15]

[10] The White House, 'National Cyber Strategy of the United States of America', 21.
[11] U.S. Department of Defense, 'Department of Defense – Defense Science Board Task Force on Cyber Deterrence' (Washington, D.C: Department of Defense, 2017), https://www.hsdl.org/?view&did=799190.
[12] Thomas Rid, 'Deterrence beyond the State: The Israeli Experience', *Contemporary Security Policy* 33, no. 1 (1 April 2012): 127–28, https://doi.org/10.1080/13523260.2012.659593; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 212–28.
[13] Rid, 'Deterrence beyond the State', 128.
[14] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008), 141–45.
[15] Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61, no. 3 (2017): 384, https://doi.org/10.1016/j.orbis.2017.05.003.

Table 1: Cases of cyber operations against the United States

Operation name	Year	Method and effects	Attacker	State reaction
NotPetya	2017	NotPetya encrypted and destroyed data on infected machines, rendering them unusable. The malware was initially delivered through Ukrainian tax software but spread globally within hours and destroyed millions of servers and computers. The operation caused billions of dollars of damage and brought multinational companies such as Maersk and FedEx to a standstill for weeks.	Russian military intelligence GRU	Delayed statement of public attribution; Blanket sanctions package against a number of Russian individuals and organisations for a variety of attacks that had wide-ranging effects.[16]
WannaCry	2017	WannaCry was a ransomware operation, which also spread globally within hours, affecting over 300,000 computers in 150 countries. It paralysed hospitals and GP surgeries, banks, and other businesses and cost billions of dollars in damages.[17]	North Korean military unit "Lazarus Group"	Delayed statement of public attribution to North Korea; Indictment against a North Korean hacker for multiple attacks, including also the Sony Pictures hack[18]; Blanket sanctions package against a number of North Korean hacker units, including Lazarus Group.[19]

[16] U.S. Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury', 15 March 2018, https://home.treasury.gov/news/press-releases/sm0312.
[17] BBC News, 'Cyber-Attack: US and UK Blame North Korea for WannaCry', *BBC News*, 19 December 2017, http://www.bbc.co.uk/news/world-us-canada-42407488.
[18] Lisa Vass, 'North Korean Programmer Charged for Sony, WannaCry Attacks and More', *Naked Security by Sophos* (blog), 10 September 2018, https://nakedsecurity.sophos.com/2018/09/10/north-korean-programmer-charged-for-sony-wannacry-attacks-and-more/.
[19] U.S. Department of the Treasury, 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups', U.S. Department of the Treasury, 13 September 2019, https://home.treasury.gov/news/press-releases/sm774.

Democratic National Committee (DNC) hack and election interference	2016	An intrusion into the DNC's network provided access to the DNC's research on Republican presidential candidate Donald Trump and emails and correspondences between DNC officials. Over the course of the 2016 presidential campaign, DNC correspondence was leaked through intermediaries such as WikiLeaks and fake persona Guccifer 2.0, leading to resignations of DNC officials. The perpetrators also hacked the email account of John Podesta, chairman of Hilary Clinton's campaign, and released more compromising information throughout the summer of 2016. Additionally, the operation involved a sweeping disinformation campaign to influence American voters and undermine confidence in the election.[20]	Russian military intelligence GRU, Russian foreign intelligence SVR, Russian Internet Research Agency	Delayed statement of public attribution; Diplomatic sanctions (expulsion of 35 diplomats and closure of 2 Russian compounds); Economic sanctions; Indictment of officials of the Russian military intelligence agency.[21]
Sony Pictures hack	2014	A breach of the networks of Sony Pictures Entertainment caused extensive physical damage to over 70% of Sony's computing infrastructure. The perpetrators stole terabytes of confidential information, which was then released online to shame Sony's management.[22] The campaign was one of coercion designed to intimidate Sony into not releasing a satirical film about North Korea's leader Kim Jong Un.[23]	North Korean military unit "Lazarus Group"	Statement of public attribution; Sanctions on three North Korean organisations and 10 individuals. (The sanctions were largely symbolic in nature given very limited trade between North Korea and the United States.[24])

[20] Robert S. Mueller III, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election' (Washington, D.C.: U.S. Department of Justice, March 2019), https://www.justice.gov/storage/report.pdf.
[21] The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment', whitehouse.gov, 29 December 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.
[22] David E. Sanger and Nicole Perlroth, 'U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing', *The New York Times*, 26 April 2020, sec. World, https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.
[23] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 170–86.
[24] BBC News, 'US Sanctions North Korea over Sony', *BBC News*, 3 January 2015, sec. US & Canada, https://www.bbc.com/news/world-us-canada-30661973.

Operation Ababil: DDoS attacks on the financial sector	2011-2013	Operation Ababil was a systematic campaign of distributed denial of service (DDoS) attacks against 46 banks and institutions in the US financial sector. As a result, bank websites were repeatedly disabled. In total, the remediation costs from the attacks amounted to tens of millions of dollars.[25]	Two computer companies working on behalf of the Iranian Revolutionary Guard Corps.	Indictment (in 2016) of 7 individuals from the two companies, accused of performing computer hacking on behalf of the Iranian government.[26]
Attack on New York State Dam	2013	The attack accessed the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam in New York State.[27] The actor did not succeed in activating the sluice gate as, at the time of the breach, the dam was under repair and therefore offline.[28]	Iran	Indictment of one Iranian official as part of the 2016 indictment detailed above.[29]

[25] FBI, 'Iranians Charged with Hacking U.S. Financial Sector', Story, Federal Bureau of Investigation, 24 March 2016, https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.
[26] The United States Department of Justice, 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector', The United States Department of Justice, 24 March 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.
[27] The United States Department of Justice.
[28] Joseph Berger, 'A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case', *The New York Times*, 25 March 2016, sec. New York, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html.
[29] The United States Department of Justice, 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector'.

Table 2: Cases of cyber operations against Israel

Operation name	Year	Description	Attacker	Victim reaction
Attack on Israeli water supply and treatment facilities	2020	The operation targeted Israel's water distribution infrastructure. It was alleged by Israel that the perpetrator tried to raise chlorine or other chemicals in the water to dangerous levels.[30] If successful, the operation would have triggered fail-safes and shut down pumping stations, which would have left civilians without water, or, in the worst case, poisoned them.[31]	Iranian government hacker unit (the specific unit is not publicly known)	Cyber attack on Iran's main port facility, Shahid Rajaee Port, which resulted in significant disruption to the port's operations and commercial shipping.[32] (Note: Israel did not officially confirm its execution of the attack.)
Hamas cyber operation	2019	A Hamas "cyber offensive,"[33] the details of which are publicly not known.	Hamas cyber unit	Air strike on an empty building used by Hamas cyber operatives.[34]

[30] AP and TOI staff, '"Cyber Winter Is Coming," Warns Israel Cyber Chief after Attack on Water Systems', The Times of Israel, 28 May 2020, https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/.
[31] Mehul Srivastava, 'Israel-Iran Attacks: "Cyber Winter Is Coming"', Financial Times, 31 May 2020, https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967.
[32] Warrick and Nakashima, 'Officials'.
[33] Zak Doffman, 'Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First', Forbes, 6 May 2019, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/.
[34] Doffman.

Table 3: Cases of cyber operations against Estonia

Operation name	Year	Description	Attacker	Victim reaction
DDoS attacks on Estonian banking, government, and media websites and Internet Service Providers (ISPs)	2007	A series of large-scale, highly coordinated DDoS attacks lasting several weeks paralysed banking services, government communications, and media reporting in Estonia. The attacks were a response to the Estonian government's decision to move a Soviet-era memorial, the Bronze Soldier, from Tallinn's city centre to a military cemetery.[35]	Criminal hackers with ties to the Kremlin	No punitive response (unilaterally or through NATO).

The omission in the tables of cyber espionage, or Computer Network Exploitation Operations (CNE),[36] is deliberate as the research question of this thesis is interested in responses to attempted or achieved sabotage or subversion.[37] The reason for this is that, although espionage operations are significant to national security,[38] they are generally not regarded as activities that can be deterred. As Amy Zegart noted, "[e]spionage is nearly impossible to deter in cyberspace for the same reason it can't be deterred anywhere else: Everyone does it."[39]

1.2 Summary of the argument: the "risk society" meets cyber conflict

In relation to the research question above, this thesis presents a central empirical and a central theoretical argument. Empirically, it argues that elements of culture and historical experience underpinning risk and threat perception, whether at the national or regional level, were crucial in shaping states' different responses to major foreign cyber attacks. Specifically, the reason the United

[35] Mils Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', in *Hybrid Threats: A Strategic Communications Perspective Annex of Case Studies*, ed. Benjamin Heap (Riga, Latvia: NATO Stratcom Centre of Excellence, 2019), https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia.

[36] CNE encapsulates the access of networks and the stealing of information. Its most important feature is that it seeks to gather information, rather than manipulate or delete it. See: Jacquelyn G. Schneider, 'Deterrence in and through Cyberspace', in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Erik Gartzke (Oxford: Oxford University Press, 2019), 108.

[37] For more extensive definitions of sabotage, espionage, and subversion see: Fischerkeller and Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', 384.

[38] For example, Richard Harknett and Max Smeets have shown that cyber espionage campaigns are *cumulatively consequential* in terms of their impact on national sources of power. See: Richard J. Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies*, 4 March 2020, 2, https://doi.org/10.1080/01402390.2020.1732354.

[39] Amy Zegart, 'Everybody Spies in Cyberspace. The U.S. Must Plan Accordingly.', The Atlantic, 30 December 2020, https://www.theatlantic.com/ideas/archive/2020/12/everybody-spies-cyberspace-us-must-plan-accordingly/617522/.

States failed to punish cyber attacks meaningfully is rooted in the dominant risk paradigm, fuelled by a cultural and historical aversion to surprise and uncertainty, which guided the US approach to cyber security competitions. In the case of Estonia, the same concerns about risk impeded a response, although these did not afflict Estonia itself, but NATO. While NATO was reluctant to issue a meaningful response due to the perceived risks of the operational environment, Estonia chose to not pressure NATO for a response due to a culturally and historically engrained fear of NATO abandonment in a future crisis with Russia. Meanwhile, the reason that Israel exhibited a more robust pattern of punishing response is that policymakers were not constrained by the paradigmatic desire to avoid and minimise risk in international security competitions and therefore did not pay particular attention to the operational environment as being inherently risky. Instead, their response calculus was shaped by a historical and cultural focus on a single primary adversary as an existential threat and a far more risk-acceptant strategic culture.

The main theoretical argument of this thesis is that the "risk society" theory, initially developed by German sociologist Ulrich Beck, but with some important modifications, presents the best lens through which to explain differences in responses as a result of the operation of risk aversion or acceptance. The theoretical approach of the risk society has recently made inroads into international security studies (see section 1.3 below), although it has not yet been applied to cyber studies. Such an application is one of the central contributions of this work. Another related contribution of this thesis is to extend the theory of the risk society and develop the concept of the *threat society* to account for cases of risk tolerance and meaningful response, which Beck's work could not do because it focused solely on risk sensitive western countries (we will return to the contributions of the thesis in section 1.4).

According to Beck's theory, risk societies are states that exhibit a strong societal preoccupation with the negative side effects of industrialisation and modernisation and are driven by the desire to prevent or minimise the uncertain hazards created by these technological processes.[40] Risk societies are therefore "reflexive" in the sense that they contend with risks that are a by-product of their own actions rather than those of other parties.[41] The awareness of unintended, negative side effects of technological progress combines with existing cultural and historical factors to create in these societies widespread anxiety about diverse future scenarios.[42] Policymaking in risk societies is therefore guided by "risk thinking": considering current policy options in terms of diverse probabilistic future scenarios.[43] This thinking is characterised by a strong desire to either avoid or minimise highly uncertain future hazards

[40] Michael J. Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', *Cooperation and Conflict* 43, no. 1 (2008): 59–60, https://doi.org/10.1177/0010836707086737.
[41] Williams, 60.
[42] Ulrich Beck, *World Risk Society* (Cambridge: Polity, 1999), 143.
[43] Mikkel Vedby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century* (Cambridge: Cambridge University Press, 2006), 4; Yee-Kuang Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', *Contemporary Security Policy* 39, no. 4 (2 October 2018): 547, https://doi.org/10.1080/13523260.2018.1494670.

and dangers, careful consideration of any potential unintended consequences of the country's own actions, and an intense focus on public safety and security.[44] Risk societies also worry that risk can never be completely eliminated and therefore engage in its proactive management. Unlike the more traditional "problem-solution" approach, risk management involves reducing likelihoods of scenarios to a level deemed tolerable or as low as one can reasonably achieve.[45] Seeking to anticipate diverse future events, thinking through decisions on the basis of not what *happens* but what *might happen*, and introducing proactive measures to avert worst-case scenarios are all tell-tale signs of risk management campaigns.[46] One example of this tendency is the increasing application of the "precautionary principle" to security decision-making to justify protective measures, in the form of pre-emptive or anticipatory action, in situations where there is "a lack of evidence of harm or straightforward causal relationships."[47]

Not every highly industrialised country is a risk society, however. A particularly important insight from Beck's work is that "risk is inherently affected by politics and the culture of each state."[48] Although material realities matter in framing the risk environment, the way in which they are perceived is subjective, meaning that different societies will have different risk thresholds.[49] Accordingly, Beck adopts a "critical realist" standpoint, which assumes risks to be real but believes that social, cultural, and historical factors shape "when people decide which risks to address and how to address them."[50] In placing emphasis on subjective perception, the sociological stance on risk management departs from the one typically provided in the organisational and finance literature, where risk management involves *objectively quantifying* the "probability and severity of risks" so as to aid decisions on how to address them.[51] In other words, the risk society perspective holds that there is no single, objective way to assess risk as a function of threat (the likelihood that an asset is attacked), vulnerabilities (the likelihood of succumbing to that attack), and consequences (the adverse effects of an attack),[52] because the

---

[44] Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006), 145.
[45] Heng, 52.
[46] Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', 547; Christopher Coker, *War in an Age of Risk* (Cambridge: Polity Press, 2009), 2; Rasmussen, *The Risk Society at War*, 3–5.
[47] Heng, *War as Risk Management*, 56; European Commission et al., 'The Precautionary Principle: Decision-Making under Uncertainty.', Science for Environment Policy (Brussels, Belgium: European Commission, September 2017), http://data.europa.eu/doi/10.2779/709033.
[48] Nathan G. Garrett, 'NATO, Security and Risk Management: From Kosovo to Kandahar, by Williams, M. J.', *The Journal of Slavic Military Studies* 23, no. 3 (3 September 2010): 525–27, https://doi.org/10.1080/13518046.2010.503171.
[49] Christopher Coker, 'Between Iraq and a Hard Place', *The RUSI Journal* 151, no. 5 (1 October 2006): 18, https://doi.org/10.1080/03071840608522868.
[50] William Clapton, 'Risk in International Relations', *International Relations* 25, no. 3 (2011): 282–83, https://doi.org/10.1177/0047117811415480.
[51] Benoît Dupont, 'The Cyber-Resilience of Financial Institutions: Significance and Applicability', *Journal of Cybersecurity* 5, no. 1 (1 January 2019): 2, https://doi.org/10.1093/cybsec/tyz013.
[52] B. Wayne Blanchard, 'Guide to Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation: A Tutorial on Emergency

assessments of these likelihoods and the importance a society attaches to them are informed not only by material realities but also by cultural and historical factors (for example, the kinds of scenarios a society most seeks to avoid).

This brings us to the divergent case of Israel discussed earlier. This thesis argues that threat societies, such as Israel, are more likely to accept the risks of a meaningful response. This is because, unlike risk societies, threat societies do not focus on diverse risks and tend to instead place their attention on a particular perception of one external existential *threat* – a threat that appears to them as being imminent, estimable, and calculable and is usually constructed against a single, well-defined adversary.[53] As in the case of risks, what give these threats particular *meaning* is the cultural and historical lens through which they are viewed. For example, in Israel's case the perception of Iran as an existential threat is exacerbated by a "siege mentality," which forms part of Israel's strategic culture.[54] Thus the conditions that produce the emergence of a threat society are, as in the case of risk societies, both material and social; that is, they involve a complex interplay between material and ideational forces.

Let us continue weaving together the thesis' empirical and theoretical arguments. To do this, we must turn to the cyber domain's high level of uncertainty — inordinate even by the standards of international anarchy — which, although it in reality affects all highly networked states roughly equally, is especially problematic for risk societies. Unlike states with a higher tolerance for risk, these states will see the technical features of the cyber operational environment that create uncertainty as an obstacle to meaningful punishment.

The problem of cyber uncertainty has two main elements. First is the complex and adaptive nature of the cyber domain. It features unclear feedback loops, multiple control parameters, and indirect information sources.[55] In such a complex system, minor alterations in initial conditions of interaction can produce large changes in behavioural patterns and strategic outcomes. The potential for unintended effects is therefore great.[56] And because the environment is also highly adaptive, it generates new causal

---

Management, Broadly Defined, Past and Present' (FEMA Emergency Management Institute, 22 October 2008), 104, https://training.fema.gov/hiedu/docs/terms%20and%20definitions/terms%20and%20definitions.pdf.

[53] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London; New York: Routledge, 2010), 18–19.

[54] Heng, *War as Risk Management*, 23; Daniel Bar-Tal and Dikla Antebi, 'Siege Mentality in Israel', *International Journal of Intercultural Relations* 16, no. 3 (1 June 1992): 251–75, https://doi.org/10.1016/0147-1767(92)90052-V.

[55] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, Inc., Publishers, 1984), 86.

[56] Perrow, 3; Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge, UK: Cambridge University Press, 2016), 115.

effects that even technical experts struggle to anticipate.[57] The overall result is "chaotic behaviour"[58]: it is difficult for states to predict the failure rates of their own actions, much more so than in the conventional domain of conflict.[59]

A second problem is proliferation: the emulation and re-use of cyber capabilities by actors other than their creator.[60] The "EternalBlue" episode illustrates the problem. Developed by the US National Security Agency (NSA), the EternalBlue exploit was stolen from the NSA and leaked online by a group calling itself the Shadow Brokers. Other actors, including otherwise militarily weak states, repurposed the exploit multiple times and used it to execute widespread and damaging cyber attacks, most infamously the 2017 WannaCry and NotPetya attacks.[61] The ease of proliferation in the cyber domain has meant that weaker states and criminal groups are able to launch destructive attacks with global ramifications – something which would not be possible in the physical domain. The relative ease of proliferation, combined with the virtual nature of capabilities, also means that it is difficult for states to estimate their adversaries' cyber capabilities at any one point in time.

These defining features of uncertainty in the operational environment produce two important consequences for states' response calculus in the aftermath of a cyber attack, which risk societies find particularly worrisome. First, operational ambiguities increase the risk of misattribution of attacks and the risk that the accused perpetrator will deny his involvement. To avoid such a scenario, a risk society will seek to achieve as high a level of confidence as possible in the identity of the attacker and therefore engage in a detailed and lengthy process of attribution, to the point where a meaningful response might no longer be viable. Second, the complexity and high degree of interconnectedness between computer systems and networks means that, in addition to introducing problems of interpretation of the initial attack (victims find it hard to determine the perpetrator's intent from the effects of the operation), there is a risk that a (cyber) retaliation might entail unintended effects, including collateral damage, "blowback," or escalation.[62] Risk-averse victims may be reluctant to engage in meaningful punishment

---

[57] Saurabh Mittal, 'Special Issue: Cyber Complex Adaptive Systems: Methodologies, Paradigms, Tools and Technologies', *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 12, no. 2 (April 2015): 209, https://doi.org/10.1177/1548512915580762.

[58] Paul W Phister Jr, 'Cyberspace: The Ultimate Complex Adaptive System', *The International C2 Journal* 4, no. 2 (2011 2010): 13; Dave Clemente, *Cyber Security and Global Interdependence What Is Critical?* (London: Chatham House, 2013), 7, http://www.chathamhouse.org/publications/papers/view/189645.

[59] For a different account of how uncertainty presents a challenge for cyber deterrence see: Martin C. Libicki, 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly* 12, no. 4 (2018): 44–57.

[60] Lucas Kello, 'Les Cyberarmes : Dilemmes et Futurs Possibles', *Politique Étrangère* 4 (Winter 2014): 140–45.

[61] Raj Samani, Christiaan Beek, and Charles McFarland, 'An Analysis of the WannaCry Ransomware Outbreak', *McAfee Blog* (blog), 12 May 2017, https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/; Lily Hay Newman, 'The Leaked NSA Spy Tool That Hacked The World', *Wired Magazine*, 3 July 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

[62] While the risk of collateral damage is particularly high in the case of a cyber response, blowback and escalation can also occur in the case of a cross-domain response. For example, if a state responds to a cyber attack with sanctions, those sanctions can also have adverse effects on the state's own economy as a result of the interconnectedness of global financial systems. Similarly, a response that imposes tough sanctions can also lead an adversary to launch a damaging cyber counterattack, resulting in escalation.

for fear of causing these effects. States with a high dependency on Internet-connected infrastructure and systems, which have often been developed with scant attention to security, are particularly vulnerable to cyber escalation if an adversary responds with a counter attack, and blowback in the case that malware from a retaliatory cyber attack spreads and causes damage to the retaliator's own systems.[63] Vulnerability to cyber escalation is not, however, the factor that determines the strength of the response. If a state is a threat society, it will pay less attention to these operational characteristics and their consequences when deciding on a response, even if it is highly dependent on digital infrastructures.

As we will see in the case studies, in the United States and at NATO, a generally low societal appetite for risk combined with the characteristics of cyberspace to produce an unwillingness to accept the above risks associated with responding to hostile cyber activity. This in turn informed the United States' and Estonia's response calculus in the aftermath of attacks (although in very different ways) and created a reluctance to issue meaningful punitive responses. By contrast, Israel, a risk-acceptant threat society preoccupied with deterring what it perceived to be an imminent existential threat from Iran, did not view the uncertainty created by the operational characteristics of cyberspace as an obstacle to meaningful responses.

The causal framework yields observable implications. If the argument of this thesis is correct, we expect to observe risk societies not punishing attacks meaningfully, primarily due to risk sensitivities with regard to the operational environment. We also expect threat societies to issue meaningful punishments for cyber attacks, while either not paying attention to the risks of the operational environment or recognising the environment as risky but choosing to accept the risks. Threat societies will pay more attention than risk societies to the perceived necessity of strongly confronting external threats, which to threat societies seem existential. It is important to note, however, that a threat society embedded in a larger risk community (such as the NATO alliance) will abide by the risk sensitivities of that community if it perceives the community to be necessary for the threat society's survival; in other words, the threat society will respond to cyber attacks as if it were a risk society – but for very different reasons that risk society, namely, involving the fear of the risk community's abandonment in a future conflict against the existential threat. If the argument is incorrect, then we should observe different response outcomes: a risk society would issue a meaningful punishment despite the recognition of operational risks; a self-standing threat society (one not in a risk community) would fail to punish cyber attacks for reasons of risk sensitivity despite the presence of a perceived existential threat; and a threat society embedded in a risk community would issue a meaningful punishment despite the fear of abandonment by the risk community.

It should be noted here that although it is near impossible to ascertain whether the absence (so far) of cyber attacks above the threshold of what International Law terms the "use of force" is due to

[63] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 189.

the fact that states are deterred from such action or due to some other cause, such as disinterest,[64] we would expect a risk society to punish attacks above this threshold. In fact, such an external shock might even have the effect of shifting the country's risk orientation – as we will see in Chapter 2, according to the sociological literature, risk societies were produced through an interaction of shock real world events (such as the September 11th terrorist attacks) and existing cultural values. As such, real world events might also trigger a risk society's transformation back into a threat society, depending on the perception of these events (through a cultural and historical lens). However, these questions are beyond this thesis's scope, which covers responses to major cyberattacks below the use of force threshold.

1.3 The risk society theory in international security studies

The conceptual approach of this thesis draws particular inspiration from the work of Christopher Coker, Mikkel Vedby Rasmussen, Yee-Kuang Heng, and Michael J Williams.[65] These scholars successfully employed the insights of Beck and other risk sociologists to the study of strategic and security affairs. Coker's main argument was that war has evolved into an *exercise in risk management*, as the principles of the risk age have led western societies and policymakers to re-conceptualise security in completely new ways.[66] He observed a paradox: while western countries have grown increasingly risk-averse, many other societies have become more willing to take greater risks.[67] In a similar vein, Rasmussen argued that in the contemporary strategic environment there is a new strategic rationality at play, centring on risk, and this has replaced Clausewitzian means-ends rational explanations.[68] Instead of defeating concrete threats to achieve perfect security, western strategy has become a way of managing risks.[69] Heng also used a thematic matrix of risk management to investigate the motivations behind and the conduct of the 1998 Kosovo war, the 2001 intervention in Afghanistan, and the 2003 Iraq war.[70] Williams argued that differences in risk perception accounted for tense transatlantic relations within NATO since the end of the Cold War.[71]

The global security environment has of course shifted since the "war as risk management" literature was created in the late 2000s. Great power rivalry has returned to the fore alongside the continued existence of ambiguous transnational risks, such as terrorism, ethnic conflict, and organised

[64] Lindsay, 'Tipping the Scales', 54.
[65] Coker, *War in an Age of Risk*; Heng, *War as Risk Management*; Rasmussen, *The Risk Society at War*; Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*.
[66] Coker, *War in an Age of Risk*, x.
[67] Coker, x.
[68] Rasmussen, *The Risk Society at War*, 8.
[69] Rasmussen, 11.
[70] Heng, *War as Risk Management*, 58.
[71] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 2.

crime.[72] Interestingly, however, despite the apparent changes in the security environment relating to the primary threat actors, this thesis finds that the lens through which the United States and NATO address security challenges in the cyber domain are strikingly similar to the way in which they approached the challenge of transnational terrorism. In other words, many of the practices, policies and ways of thinking employed in the 2000s are being adapted by western policymakers to the realm of cyber conflict.

1.4 Theoretical and empirical contributions of the thesis

The risk society theory has not yet been employed to shed light on states' decision-making in responding to offensive cyber operations. In this thesis, the risk framework in Chapter 2 and Chapter 3 will contribute to second level constructivism in International Relations, which focuses on the importance of ideas and beliefs of individual countries and regimes in generating international outcomes. The framework will show how cultural beliefs and historical experience producing risk aversion or risk acceptance interact with the material environment to produce particular international outcomes in state responses to cyber attacks. More specifically, to explain how risk *aversion* produces weak responses, the framework will take as a starting point Beck's theory, which posits that technological progress interacts with western culture and western historical experience to produce societal risk sensitivity. The thesis will extend this theory to cyber issues, proposing that the risk sensitivity present in certain societies permeates cyber related decision-making in particular as the cyber domain is an environment of inherent uncertainty, which produces weak responses. To explain how risk *acceptance* produces meaningful responses, the thesis will conceptually refine the theory of the risk society by developing the concept of the *threat society*. It will show that cultural factors (particularly strategic culture) and historical experience produce perceptions of a single adversary as an existential threat, which overshadows any concerns about the uncertainty of the operational environment, producing meaningful responses to cyber attacks.

This framework based on second level constructivism is particularly valuable for answering the research question of the thesis because it is able to account for *variation* in states' responses to cyber attacks, which, as we will discuss in Chapter 2, systemic theories cannot do in the context of the case studies analysed here. It is also able to explain why different state leaders, representing very different political views, came to the same decisions, and why the United States, Israel, and Estonia, despite sharing liberal democratic values and being equally embedded in networks of co-dependence, responded to cyber attacks differently. By integrating both material factors and social construction, this thesis proposes a unique and original conceptual framework for understanding policymakers' seemingly disparate explanations for responses to cyber attacks, thus solving the research puzzle set out in this

[72] Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', 545.

chapter. In so doing, the thesis aspires to empirically contribute to the central aim of security studies as a sub-discipline: "to interpret, explain, or predict interstate behaviour" in security competitions.[73] Looking at the puzzle of states' responses to cyber operations through the lens of the risk society will also contribute to the development of research agendas that are focused on "technical-functional knowledge issues," which helps redress the imbalance of attention devoted to such issues in comparison to what Jarvis and Griffiths called the "grand questions of IR [International Relations]," such as the causes of war or American hegemony.[74]

The final contribution of this thesis to IR scholarship is building bridges between the disciplines of International Relations (IR), Sociology, and Computer Science. Indeed, International Relations and the sub-discipline of international security studies draw on contributions from other disciplines.[75] This is exemplified in Kenneth Waltz's "Theory of International Politics", which utilises concepts from macroeconomic theory to illuminate interstate dynamics, and Thomas Schelling's work integrating theoretical models from mathematics into strategic studies.[76] The influence of Sociology on International Relations is also clearly visible through the popularity of social constructivist theories and critical IR theory.[77]

Despite this influence of Sociology on IR, in an introduction to a special issue on the study of risk in IR, Hameiri and Kühn pointed out that academic literature on the subject is only fledgling, which is all the more surprising because, as the authors showed, for the past two decades risk management has guided government policymaking on issues from counter-terrorism to financial regulation and public health.[78] Much of the study of risk in IR has additionally been dominated by an ontological debate between those who view risks as grounded in material reality, following the work of Ulrich Beck and Anthony Giddens, and critical scholars who view risks as entirely socially constructed, influenced by the work of Mary Douglas and Michel Foucault.[79] Hameiri and Kühn therefore called for more scholarly analyses to examine issues in world politics through sociological perspectives on risk.[80] On the cyber front, Lucas Kello also believes that a "Congress of Disciplines" is urgently needed to interpret the

[73] Kello, *The Virtual Weapon and International Order*, 132.
[74] Darryl S. L. Jarvis and Martin Griffiths, 'Learning to Fly: The Evolution of Political Risk Analysis', *Global Society* 21, no. 1 (2007): 2, https://doi.org/10.1080/13600820601116435.
[75] Heng, *War as Risk Management*, 16.
[76] Kenneth N. Waltz, *Theory of International Politics* (New York ; London: McGraw-Hill, 1979); Schelling, *Arms and Influence*.
[77] Darryl S.L. Jarvis and Martin Griffiths, 'Risk and International Relations: A New Research Agenda?', *Global Society* 21, no. 1 (1 January 2007): 1–4, https://doi.org/10.1080/13600820601116427; Jarvis and Griffiths, 'Learning to Fly'; Shahar Hameiri and Florian P. Kühn, 'Introduction: Risk, Risk Management and International Relations', *International Relations* 25, no. 3 (2011): 275–79, https://doi.org/10.1177/0047117811415479; Clapton, 'Risk in International Relations'.
[78] Hameiri and Kühn, 'Introduction', 275.
[79] Hameiri and Kühn, 276–77.
[80] Hameiri and Kühn, 278.

consequences of cyber technologies for international security.[81] This thesis, in drawing on multiple disciplines and examining cyber issues through the lens of risk, is an answer to both these calls.

Finally, in terms of policy contributions, the analysis here aims to provide policymakers with a greater awareness of how societal dispositions towards risk influence their decisions on cyber issues. This knowledge in turn can help them develop strategies of cyber conflict prevention that might be better suited to societal and cultural dispositions, thereby increasing the chances of successful implementation.

1.5 Methods and data

This section will first explain why the thesis has taken a case study approach as its primary methodology, followed by a justification of the case selections. It will then discuss the sources of primary data and the limitations of the qualitative methodology.

1.5.1 Case study approach

John Gerring defined a case study as an in-depth study of a single unit where the scholar's aim is to elucidate features of a larger class of similar phenomena.[82] The essence of a case study is that it tries to "illuminate decisions": why they were taken, how they were implemented, and what was the result.[83] By focusing on states' decisions, therefore, the central research question of this thesis lends itself to this method. Each empirical chapter will apply the framework elaborated in Chapters 2 and 3 to each of the cases for the purposes of answering the research question.

Generally speaking, qualitative reviews of single cases are better suited to cyber studies than large quantitative surveys due to the barriers of data collection, which hinder quantitative studies more than they do qualitative studies.[84] There are tens of thousands of cyber breaches reportedly occurring each day, and, while the vast majority of these incidents will be low-level operations of little significance to national security, the validity of inferences from quantitative studies, which rely on an accurate picture of a whole universe of events, may suffer.[85] Deep analyses of single cases, by contrast, can expose new facts about known events and highlight effects that have previously been unexplored. This, in turn, can also help identify patterns that defy trends in conventional statecraft.[86]

---

[81] Kello, *The Virtual Weapon and International Order*, 42.
[82] John Gerring, *Case Study Research: Principles and Practices* (Cambridge, UK: Cambridge University Press, 2016), 28.
[83] Robert K. Yin, *Case Study Research and Applications: Design and Methods*, Sixth Edition. (Thousand Oaks, California: SAGE Publications, Inc, 2018), 14.
[84] Kello, *The Virtual Weapon and International Order*, 40.
[85] Kello, 40.
[86] Kello, 40–41.

1.5.2 Case selection

The thesis investigates responses to individual cyber incidents as part of larger country case studies. The cases were selected according to their risk society or threat society identity. Briefly, risk societies are those that demonstrate reflexivity (a concern with the unintended side effects of technological progress), are preoccupied with risks (diverse, potential, worst-case scenarios that are often an unintended consequence of a decision or action) and have a tendency to handle security issues using risk management practices. As we already mentioned, in the case of the United States, the sociological literature and security studies literature posits that the United States is a risk society – hence its selection for this study. Threat societies exhibit a willingness to accept risks, seek self-reliance, and are preoccupied with what they perceive to be imminent existential threats. Both Israel and Estonia were found to fit this description. The particular selection of Estonia was motivated by the fact that Estonia is also part of NATO, which, according to the risk society literature, is a "risk community," an alliance dominated by risk societies.[87] The value of Estonia for this thesis is therefore in examining the determinants of responses of a threat society embedded in a risk community.

The cases were also selected due to their similarities in several important respects. All three states are democracies with shared liberal values – thus the variable of regime type was kept constant across the case studies. All three are also highly industrialised and enormously dependent on digital technologies and cyberspace for the everyday functioning of their societies; they are therefore equally vulnerable to severe disruption resulting from cyber attacks. All three countries have also fallen victim to cyber attacks that reached the threshold of significance for national security, as Tables 1, 2, and 3 in this chapter evidenced.

On a practical level, the case studies are accessible thanks to policymakers' knowledge of the English language (all the interviews were conducted in English without the need for an interpreter) and the existence of English language policy documents. The cyber attacks that these states have experienced are also well-documented by journalists and government agencies. In short, there is enough information in the public domain to allow for rigorous study of these national contexts, which is unique given the often covert and clandestine nature of cyber operations.

An instinctive reaction to any juxtaposition of Israel and the United States might be to point out that Israel's geopolitical environment is very different to that of the United States – indeed, with the exception of a small number of countries (such as Egypt and Jordan), Israel's regional neighbours still don't officially recognise the country's sovereign existence. While the variable of the geopolitical environment cannot be dismissed at this stage, the Israel case study in Chapter 5 will show that it was

[87] Christopher Coker, *Globalisation and Insecurity in the Twenty-First Century: NATO and the Management of Risk*, Adelphi Papers; No. 345 (Oxford and New York: Oxford University Press for the International Institute for Strategic Studies, 2002).

not the geopolitical environment alone or even primarily that shaped Israeli reactions – instead, it was the interplay of material and ideational factors, particularly *perceptions* of Israel's main adversary Iran as an existential threat, which were in turn a product of strategic culture and historical experience.

There are also important reasons to suggest that Israel and the United States might take similar approaches towards the cyber domain. Israel is a close ally of the United States and the two have collaborated in the context of prominent cyber operations. There is strong evidence, for example, that the highly sophisticated Stuxnet attack on the Natanz nuclear plant in Iran between 2005 and 2010 was a joint effort between the United States and Israel.[88] Despite their alliance, however, Israel and the United States responded to cyber attacks in starkly different ways.

1.5.3 Data collection

Case study research relies on multiple sources of evidence and the triangulation of data.[89] The three case studies will rely on primary data derived from a number of sources to allow for such data triangulation. The analysis will use thirty-seven interviews conducted by the author with policymakers and their senior advisers; policymakers' memoirs; official statements and speeches; interviews in the media; press releases and briefings; official government documents (including doctrines and strategies); government reports; unsealed indictments; leaked information and leaked diplomatic cables; private sector threat intelligence reports; investigative reporting from credible news outlets; and congressional and committee testimonies. Most important for assessing how decisionmakers perceived the operational environment will be personal interviews conducted with policymakers and individuals who were close to the response decision-making processes.

The data sources identified above present obstacles of data collection and reliability. Relying on public statements from policymakers has pitfalls. Such public declarations cannot always be taken at face value: there is always the possibility that policymakers might be advancing their own agendas or seeking to portray themselves in a certain way; possibly, their intentions and motives are the opposite of what they publicly declare.[90] To address this problem, the thesis will use multiple data sources, giving special attention to interview data.[91]

A second methodological limitation of the analysis of the thesis is the possibility that states' responses to cyber incidents were covert and thus took place outside the public domain. There is no clear way to completely eliminate this barrier. There are two important caveats to the issue of covertness, however, which can help to mitigate the implications of this obstacle. First, as Chapter 3

[88] Kim Zetter, 'The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks', *Wired*, 2 October 2015, https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/.
[89] Yin, *Case Study Research and Applications*, 15.
[90] Heng, *War as Risk Management*, 15.
[91] Heng, 16.

will discuss at greater length, the interconnectedness of systems in the cyber domain means that there is a high degree of probability that an offensive cyber operation will end up spreading outside its target (even the aforementioned highly sophisticated and targeted Stuxnet malware ended up spreading outside the Natanz nuclear plant).[92] If this is the case, the operation is likely to be picked up by private threat intelligence companies, which regularly survey the landscape for new strands of malware and report publicly on their findings. In other words, a significant retaliatory cyber operation would most likely enter into public knowledge. Second, there is a strong argument that responses that are public are more meaningful as they build credibility. This is particularly the case if an incident has been attributed publicly, that is, if a state has publicly declared another state actor to be responsible for a damaging cyber operation and promised to follow up with punishment – failure to administer this punishment leads to the state appearing weak in the eyes of the international community. Jack Goldsmith and Robert Williams elaborated on this point further with reference to the United States, writing that, "[e]ven if the United States is robustly engaging in retaliatory covert or clandestine responses, those responses cannot contribute to deterrence against the many third parties who are watching, and indeed in context detracts from it … Unless a nation is able to effectively redress a cyber intrusion, it can be harmful or self-defeating to publicize it, since public knowledge of loss and the failure to respond effectively invite more attacks."[93]

1.6 Structure of the thesis

Having discussed the research puzzle, the empirical and theoretical contributions of the thesis, and the methodology, we now turn to mapping out the remainder of the thesis. *Chapter 2* will first consider how alternative theoretical schools in IR might approach the research puzzle of this thesis. It will then position the theoretical framework, the risk society, under the broad heading of constructivist approaches in International Relations and discuss the risk society literature. As part of this review, the chapter will develop the concept of the threat society as an important refinement of the risk society theory. *Chapter 3* will examine how risk societies will react to the uncertainties inherent in cyberspace by examining the relationship between intervening variable – the cyber operational environment – and the causal mechanism – the perception of this environment by risk societies.

---

[92] Stuxnet did not, however, release its destructive payload outside the systems it targeted. For further elaboration of this case see: Monica Kaminska, Fabio Cristiano, and Dennis Broeders, 'Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone', in *13th International Conference on Cyber Conflict: Going Viral*, ed. Tatiana Jančárková et al. (Tallinn, Estonia: NATO CCDCOE Publications, 2021).

[93] Jack Goldsmith and Stuart Russell, 'Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations' (Stanford, CA: Hoover Working Group on National Security, Technology, and Law, 5 June 2018), 13, https://lawfareblog.com/strengths-become-vulnerabilities-how-digital-world-disadvantages-united-states-its-international-0.

Chapter 4 will be dedicated to the first case study, the United States, which will argue that the avoidance of risk, particularly the risk of escalation, was the most important factor in producing weak responses to cyber attacks. It will start with a historical overview of significant cyber incidents that have afflicted the United States and show that, while all the attacks created significant effects for national security, they were all met with weak punitive responses. Next, the chapter will discuss the societal, historical, and cultural factors that contributed to the development of the risk society in the United States. Having "set the scene," the chapter will discuss policymakers' perceptions of cyberspace under the Obama and Trump administrations and examine whether these perceptions and considerations of risks, including the risk of misattribution and the risk of unintended effects, influenced the decision-making processes on responses. The final substantive section of the chapter will consider whether the United States adopted risk management practices in the cyber domain.

Chapter 5 will consider the case of Israel, arguing that Israeli strategic culture determines Israel's nature as a threat society, which in turn shapes Israel's responses to cyber attacks. As before, the chapter will begin with an overview of the most significant cyber attacks that Israel fell victim to, but this time show how the Israeli government issued meaningful punishments. The chapter will then analyse particular features of Israeli strategic culture that create the threat society and explain how they influence Israeli deterrence strategy and the perception of its main adversary, Iran, as an imminent survival threat. The analysis will seek to show that Israel's threat society identity, by shaping Israel's deterrence strategy and its view of Iran, also produced Israel's meaningful responses to cyber operations. The final section of the chapter will analyse practices that Israel carried out alongside meaningful punishment, focusing particularly on prevention as part of the "campaign between wars," and explaining its place in Israel's deterrence strategy.

Chapter 6 will focus on the case of Estonia and show that, although Estonia itself was a threat society due to its ongoing preoccupation with the perceived existential threat posed by Russia, Estonia's beliefs regarding its precarious position within NATO, NATO's sensitivity to the risks of the operational environment and the risks of tensions with Russia, and Estonia's fear of alliance abandonment in a future crisis scenario, meant that it did not pressure NATO to initiate formal proceedings against Russia. Structurally, the chapter will start with an overview of the 2007 cyber attacks and illustrate their relevance to national security. It will then show that Estonia's threat society identity was a result of its historical perception of Russia as an existential threat and Finnish-inspired strategic culture, which encouraged a "fighting spirit." The chapter will explain that Estonia's threat sensitivity to Russia was so strong that it decided to pursue two defence models simultaneously to ensure full redundancy: the Finnish total defence model and collective defence under NATO. Having set the context for Estonia's decision-making in 2007, the chapter will then turn to investigating why Estonia chose not to invoke any of NATO's collective defence articles in response to the DDoS attacks. The final section will examine whether, as a result of the attacks, Estonia in later years became more reflexive as a society and whether it moved up the risk spectrum. It will conclude that the country in fact remained a threat

society due to its continued firm focus on the Russian existential threat through a historical and strategic cultural lens.

Chapter 7 will conclude the thesis by comparing and contrasting the findings from the case studies and discussing the contributions of the thesis to International Relations scholarship. The chapter will also discuss the implications of the findings for the field of cyber studies and for cyber-related policy, and briefly evaluate recent developments lying outside the timeframe of the thesis. The chapter will conclude the thesis with suggestions for further research.

Chapter 2
Conceptual Framework: The Risk Society

2.1 Introduction

This chapter presents a conceptual framework which will orient the empirical chapters' explanation of state responses to offensive cyber operations.[1] The framework draws from and adapts concepts from the "risk society" theory within Sociology[2] and the "war as risk management" literature in International Relations (IR).[3] The theory of the risk society sheds light on the origins of western risk sensitivity as linked to technological progress and cultural factors, and showcases the enormous importance of attitudes towards risk for international outcomes. The theory is especially pertinent to the investigation of state responses to cyber attacks because, as we will see in Chapter 3, the cyber domain, due to its virtual nature and other technical features, entails a particularly high level of operational uncertainty, leaving a wide berth for interpreting conceivable worst-case scenarios. Highly risk sensitive societies are especially prone to considering diverse worst-case scenarios, which tends to paralyse their decision-making and eventually leads them to adopt preventive measures. Cyber conflict for risk societies also epitomises their reflexive concerns about the negative side effects of technological progress: once considered an engine of economic growth, cyberspace is now seen as a realm of national security risk. Societies low in risk sensitivity are usually those that perceive their security landscape to be dominated by a threat to survival from one particular actor, which means that their decision-making is motivated by a single scenario that effectively performs the role of a heuristic. Such societies devote far less attention to the nature of the operational environment, focusing instead on the perceived historical and ideological threat of their main adversary.

As a preliminary step to the theoretical discussion, the chapter will first consider the strengths and limitations of rationalist theories and other alternative theoretical approaches in IR regarding the empirical puzzle of the thesis. The discussion will focus on two rationalist theories – neorealism and neoliberalism – as well as cognitive and psychological approaches. It will explain the main tenets of

[1] Parts of this chapter were published in: Monica Kaminska, 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks', *Journal of Cybersecurity* 7, no. 1 (9 March 2021), https://doi.org/10.1093/cybsec/tyab008.

[2] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE, 1992); Anthony Giddens, 'Risk Society: The Context of British Politics', in *The Politics of Risk Society*, ed. Jane Franklin (Cambridge: Polity Press, 1998); Ulrich Beck, *World Risk Society* (Cambridge: Polity, 1999).

[3] Christopher Coker, *War in an Age of Risk* (Cambridge: Polity Press, 2009); Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006); Mikkel Vedby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century* (Cambridge: Cambridge University Press, 2006); Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London ; New York: Routledge, 2010).

these theories and highlight areas where they fall short analytically. The last part of the section will discuss constructivism and position the risk society theory within the broad umbrella of constructivist thinking. The remainder of the chapter will review the risk society literature, discuss the origins of the risk society theory, offer a definition of risk, and refine the risk framework to include the new concept of the *threat society*.

The analysis of this chapter will guide the empirical investigation of ensuing chapters, which seek to show that societies' desire for risk minimisation, or lack thereof, explain their different responses to foreign cyber attacks. In so doing, it will provide the basis for the main empirical arguments of this thesis: that the United States failed to punish cyber attacks meaningfully because as a risk society it was unwilling to accept the risks inherent in the operational environment; that Estonia – although itself not a risk society – in being a member of the NATO "risk community," yielded to the risk sensitivities of NATO, which it perceived (through its threat society lens) to be key to the nation's long-term survival; and Israel, unconstrained by "risk thinking" due to its peculiar strategic culture, which encouraged risk-taking and produced a myopic focus on the state's physical survival, especially against the existential threat from Iran, paid less attention to the operational environment as an obstacle to punishment – and thus was more willing to respond credibly to cyber attacks.

2.2 Existing literature

Few studies of state responses to foreign cyber attacks exist within International Relations. Nevertheless, we can evaluate the analytical applicability and shortcomings of existing theoretical approaches in relation to the empirical puzzle of this thesis. In particular, this section will review neorealism, neoliberalism, cognitive and psychological approaches, and constructivism. It will identify the strengths and weaknesses of those approaches; later we will explore how the risk society framework coupled with constructivism can help fill those gaps. Overall, we will see that constructivism supplies the best theoretical foundations for resolving the empirical puzzle. Constructivism is not without its own limitations, however. The risk society framework helps to overcome them.

2.2.1 Rational choice theories

As rational choice theories, neorealism and neoliberalism share important characteristics: states are understood to be unitary actors; their behaviour reflects their purpose or intention; and actions are chosen on the basis of a calculated solution to a strategic problem (that is, a rational cost-benefit analysis).[4] Utility maximisation is understood by rational choice theories as the ultimate aim of foreign

[4] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999), 15; Stephen M. Walt, 'Rigor or Rigor Mortis?: Rational Choice and Security Studies', *International Security* 23, no. 4 (1999): 10.

policy decision makers.[5] The Rational Actor Model, in seeking to explain state behaviour, first considers what goal a government was pursuing and whether it had the ability to achieve that goal, and then seeks to explain how a particular decision was a rational choice in light of that goal.[6] The rational choice approach also considers the constraints under which an actor makes decisions, which may be technological, institutional, or arising from interdependencies.[7] Rational choice theories assume that humans are "instrumentally rational": given existing preferences, they will engage in ends-means calculations.[8] Rational choice has served as the bedrock of numerous theories of foreign policy decision-making in the security realm, including Schelling's game theoretical approach to the dynamics of nuclear deterrence and James Fearon's theory of how intentional misrepresentation of information about capabilities and resolve might lead states to go to war.[9]

According to rationalist approaches, interests are exogenously defined and "logically prior to any beliefs held by the actors."[10] For both neorealism and neoliberalism, these prior interests are material – the theories maintain that the pursuit of material interests drives state behaviour in the anarchic states system. According to Stephen Walt, such theories that rely on strong assumptions about each actor's preferences are a form of "thick rationality."[11] Let us now review our two sample rationalist approaches in IR, neorealism and neoliberalism, and explore how they might address the puzzle of state responses to cyber attacks.

A) Neorealism

Neorealism emphasises the international system's anarchic nature in determining general trends in international security competition. It also emphasises the relative distribution of military power across units (states).[12] The structure of the international system will, according to neorealism, constrain states in certain actions and incentivise others.[13] It predicts that states will seek to redress imbalances

---

[5] Chris Alden, *Foreign Policy Analysis: New Approaches*, Second edition. (Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2017), 20.
[6] Allison and Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 15; Duncan Snidal, 'Rational Choice and International Relations', in *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse-Kappen, and Beth A. Simmons (London; Thousand Oaks, CA: SAGE Publications, 2013), 87, https://ezproxy-prd.bodleian.ox.ac.uk/login?url=http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=1046504.
[7] Snidal, 'Rational Choice and International Relations', 87.
[8] Janice Gross Stein, 'Decision Making: Rational, Psychological, and Neurological Models', in *Foreign Policy Theories Actors Cases*, ed. Steve Smith, Amelia Hadfield, and Tim Dunne (Oxford: Oxford University Press, 2012), 132.
[9] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Massachusetts: Harvard University Press, 1960), 17; James D. Fearon, 'Rationalist Explanations for War', *International Organization* 49, no. 3 (1995): 379–414.
[10] Judith Goldstein and Robert O. Keohane, *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change* (Ithaca: Cornell University Press, 1993), 4.
[11] Walt, 'Rigor or Rigor Mortis?', 11.
[12] Kenneth N. Waltz, *Theory of International Politics* (New York ; London: McGraw-Hill, 1979).
[13] Kenneth N. Waltz, 'Realist Thought and Neorealist Theory', *Journal of International Affairs* 44, no. 1 (1990): 29.

of power in the international system such that no single state or group of states can control it. A number of variations in the distribution of power are conceivable, for example, multipolarity, bipolarity, and unipolarity.[14] In the interest of parsimony, neorealism intentionally neglects any consideration of the internal characteristics of states, such as culture or ideology, or of individuals in those states.[15] In short, it is a "third-level" or systemic theory.

Kenneth Waltz, the school's founder, has been described as a "defensive" neorealist due to his belief that, "[i]n crucial situations, the ultimate concern of states is not for power but for security."[16] State behaviour, according to this approach, is driven primarily by concerns for survival. Absent any higher authority, states will be incentivised to constantly be on the lookout for potential threats to their national security, while simultaneously seeking to maximise it. This leads to what defensive neorealists call the security dilemma: "many of the means by which a state tries to increase its security," wrote Robert Jervis, "decrease the security of others."[17] The security dilemma will be particularly intense in two situations: when defensive capabilities cannot easily be distinguished from offensive capabilities and, second, when geographical factors and developments in military technology favour offensive action rather than defensive action.[18]

Neorealism also has an offensive variant, of which John Mearsheimer is a prominent proponent.[19] His approach differs from defensive neorealism in that he believes that states not only seek security to ensure survival, but instead, they seek power maximisation, which means that rather than being incentivised to maintain an existing balance of power, states wish to revise it to their advantage.[20] They are locked into a perpetual competition to gain power at each other's expense. Each state not only aims to become the strongest in the international system; they also aspire to hegemony – to being "the only great power in the system."[21] This leads Mearsheimer to posit that multipolar systems are less stable than bipolar systems; and multipolar systems that contain especially powerful states are the most war-prone of all.[22]

Applying neorealist tenets to understanding international developments related to the cyber domain is difficult. Neorealism's prioritisation of physical survival and military power means that it cannot readily accommodate capabilities that are non-physical in nature and which do not overtly threaten the physical survival of the state. And yet, cyber capabilities still bear material effects and are

[14] Joseph S. Nye, 'Neorealism and Neoliberalism', ed. Robert O. Keohane and Richard Rosecrance, *World Politics* 40, no. 2 (1988): 241, https://doi.org/10.2307/2010363.
[15] John Glenn and Darryl Howlett, 'Neorealism', in *Neorealism versus Strategic Culture*, ed. John Glenn, Darryl A. Howlett, and Stuart Poore, Critical Security Series (Abingdon, Oxon ; New York, NY: Routledge, 2018).
[16] Waltz, 'Realist Thought and Neorealist Theory', 36.
[17] Robert Jervis, 'Cooperation under the Security Dilemma', *World Politics* 30, no. 2 (1978): 169, https://doi.org/10.2307/2009958.
[18] Jervis, 'Cooperation under the Security Dilemma', 186–94.
[19] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York ; London: Norton, 2001).
[20] Mearsheimer, 20.
[21] Mearsheimer, 2.
[22] Mearsheimer, 5.

thus consequential for national security.[23] While cyber capabilities have not (yet) been used in an attack that would produce death and destruction equivalent to a conventional military strike, they have produced significant political, social, and economic effects, which has resulted in their prominent position among the top security concerns of states.[24] Yet, theoretical models which focus on physical coercion and territorial conquest are not immediately able to make sense of reactions to aggression which falls below the threshold of use of force.[25]

In the context of our research puzzle, a neorealist sceptical of the potential for cyber means to inflict levels of damage that would rise to a national security threat might suggest that the United States and Estonia did not respond to hostile cyber operations because these did not *merit* a response. The effects of the cyber operations to which these countries fell victim, this view might hold, had no significance for the broad distribution of power in the international system. And since it is the distribution of power that dictates general trends in state behaviour, it is no surprise that neither the United States nor Estonia failed to respond meaningfully. The same neorealist, however, would have trouble accounting for the behaviour of Israel – a state that retaliated against foreign cyber attacks (with a cyber attack on Iran's Shahid Rajaee port, for example). If cyber operations do not threaten the state's physical security or survival enough to warrant a meaningful response, then why did Israel respond so strongly? Moreover, neorealism struggles to account for why states continually stress the national security implications of cyber hostilities in official policy statements. Already in 2010, the US National Security Strategy claimed that "[c]ybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[26] Since then, every national security strategy has advanced the same notion.[27]

Neorealism's emphasis on exogenously given material interests leads it to miss the importance of another important driver of state responses to cyber attacks: cultural and ideational factors. As the empirical chapters of this thesis will show, because the cyber operational environment is inherently uncertain, it increases the possibilities for subjective interpretation of possible conflict scenarios. This opens up the way for cultural and historical biases to shape decision-making outcomes in a cyber conflict, which helps to account for variation in national responses.

---

[23] For a discussion of how cyber campaigns are strategic in intent and can they can affect sources of national power see: Richard J. Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies*, 4 March 2020, 1–34, https://doi.org/10.1080/01402390.2020.1732354.
[24] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 55; Office of the Director of National Intelligence (ODNI), 'Annual Threat Assessment', 9 April 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
[25] Kello, *The Virtual Weapon and International Order*, 56.
[26] The White House, 'National Security Strategy', May 2010, 27, https://nssarchive.us/wp-content/uploads/2020/04/2010.pdf.
[27] The White House, 'National Security Strategy', February 2015, 1, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; The White House, 'National Security Strategy', December 2017, 12, https://nsarchive2.gwu.edu//dc.html?doc=4421220-The-White-House-National-Security-Strategy-of.

B) Neoliberalism

Neoliberal institutionalism posits that states are able to cooperate to achieve common interests even under conditions of anarchic uncertainty.[28] It therefore departs from the neorealist assumption that, with primary motivations of security and power measured relative to other states in the system, states cannot hope to enter into mutually beneficial cooperation agreements.[29] Neoliberals believe that in recognising the benefits of cooperation, states overcome the difficulties in the international system posed by an absence of a higher authority and develop institutions, which "provide information, reduce transaction costs, make commitments more credible, establish focal points for coordination, and … facilitate the operation of reciprocity."[30] Even particularly powerful states need international institutions to pursue their aims because the cost of exercising influence on a bilateral basis is too high.[31] They themselves tend to follow the rules of institutions because they derive a net benefit from other states following the rules in that these make states' behaviour more predictable.[32]

To illustrate, neoliberal institutionalism has been fruitfully applied to explain the persistence and continuing effectiveness of international arms control regimes, such as the conventional arms reduction regime and the operational arms control regime, after the collapse of the Soviet Union.[33] Frank Schimmelfennig showed that western states did not use their victory over the Soviet Union to impose new rules that would shift the military balance in their favour, but rather had an interest in integrating post-Soviet states into existing institutional frameworks as they understood this to be the best way of maintaining international stability and controlling uncertainties stemming from the dissolution of the Soviet Union.[34]

Neoliberal institutionalism has trouble elucidating state behaviour in the context of cyber capabilities, however. This is because the nature of cyber capabilities and cyberspace is such that cyber arms control agreements are particularly hard to establish and enforce. Offensive capabilities, which amount to lines of computer code, are easy to obscure and often dual-use in nature; their existence cannot therefore be easily verified, let alone quantified.[35] Furthermore, states have incentives not to

---

[28] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton; Oxford: Princeton University Press, 2005).
[29] Robert O. Keohane and Lisa L. Martin, 'The Promise of Institutionalist Theory', *International Security* 20, no. 1 (1995): 41–42, https://doi.org/10.2307/2539214.
[30] Keohane and Martin, 42.
[31] Robert O. Keohane, 'International Institutions: Can Interdependence Work?', *Foreign Policy*, no. 110 (1998): 83, https://doi.org/10.2307/1149278.
[32] Keohane, 86.
[33] Frank Schimmelfennig, 'Arms Control Regimes and the Dissolution of the Soviet Union: Realism, Institutionalism and Regime Robustness', *Cooperation and Conflict* 29, no. 2 (1 June 1994): 115–48, https://doi.org/10.1177/0010836794029002002.
[34] Schimmelfennig, 142.
[35] Joseph S. Nye, 'The World Needs an Arms-Control Treaty for Cybersecurity', Belfer Center for Science and International Affairs, 1 October 2015, https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity.

comply with cyber arms control regimes, because revealing the existence of capabilities could effectively render them useless, as the vulnerabilities that the code would seek to exploit could immediately be patched by potential targets. Where attempts to control hostile cyber conduct have been made, for example in 2015 when US President Barack Obama and Chinese President Xi Jinping agreed that their countries would refrain from conducting cyber theft of intellectual property,[36] they have largely failed because they lacked supporting institutional devices.[37]

More general efforts to achieve international agreement on responsible behaviour in cyberspace, such as the UN Governmental Group of Experts (UNGGE) on Responsible State Behaviour and the recently established Open Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, have been hampered by different visions of internet governance between what is known as the "likeminded group," largely western liberal democracies, on the one hand, and authoritarian regimes including Russia and China, on the other.[38] What the failure to develop effective regimes and international institutions in relation to cyber capabilities shows us is that state behaviour is highly unlikely to be influenced by such institutions. In other words, institutions and regimes are unlikely to account for patterns of response and non-response to cyber operations; the characteristics of the cyber capabilities and of the operational environment render international institutions inherently difficult to establish and operate effectively for the purposes ascribed to them by neoliberals. The absence of such institutional constraints in the cyber domain could explain the general increase in the incidence of interstate cyber attacks that we have witnessed over the last decade and a half. It does not, however, explain why some countries – such as the United States and Estonia – showed weakness in responding to such incidents, while other countries – such as Israel – responded meaningfully.

One strength of neoliberalism is found in complex interdependence theory. The theory holds that some states may find themselves in a situation of asymmetrical interdependence as a result of their economies' high reliance on global economic flows and the repeated interaction of societies.[39] When a state is deeply embedded in networks of co-dependence, this complicates calculations of power gained or lost relative to other states. One of Robert Keohane and Joseph Nye's key contributions is the observation that in those situations, states will pay attention to absolute gains, rather than just relative

[36] John W Rollins et al., 'U.S.–China Cyber Agreement' (Washington, D.C.: Congressional Research Service, 16 October 2015), https://fas.org/sgp/crs/row/IN10376.pdf.
[37] CNBC, 'US Accuses China of Violating Bilateral Anti-Hacking Agreement', CNBC, 9 November 2018, https://www.cnbc.com/2018/11/09/us-accuses-china-of-violating-bilateral-anti-hacking-agreement.html.
[38] Dennis Broeders, Liisi Adamson, and Rogier Creemers, 'A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' (The Hague: The Hague Program for Cyber Norms, 2019), https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace.
[39] Robert O. Keohane and Joseph S. Nye Jr, 'Power and Interdependence', *Survival* 15, no. 4 (1 July 1973): 159–61, https://doi.org/10.1080/00396337308441409; Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 4th ed. (Boston; London: Longman, 2012).

gains – as realists argue – thereby increasing the chances for cooperation.[40] Elaborating on these ideas with reference to the cyber domain specifically, Nye proposed that a state might be deterred from launching a cyber attack, not because the target is well-defended or due to fear of retaliation, but because of "entanglement," meaning "the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim."[41] In practice, this would mean that a retaliatory cyber attack, due to the high level of Internet-related interdependence, might have repercussions for the retaliator (a scenario commonly known as "blowback"), which might lead the retaliator to conclude that they face more material drawbacks than benefits from retaliation.

While the theory of interdependence is compelling, and indeed, as we will see in the next chapter, considerations of blowback are prominent worries in some states, the theory fails to account for variation in responses across the three case studies. The United States, Israel, and Estonia are all highly dependent on complex, Internet-connected networks crossing multiple jurisdictions, yet they responded differently. What we will see is that for the United States, sensitivity to cyberspace being a complex interdependent system of networks and the resulting potential for blowback was an important consideration in the response calculus – but puzzlingly for complex interdependence theory, this was not the case for Israel. What this thesis will instead propose is that worries about potential blowback are prominent among states that have a high sensitivity to risk – a sensitivity, which is culturally informed and which involves domestic-level considerations that neoliberalism, as a systemic theory of international relations, neglects.

2.2.2 Cognitive and psychological approaches

Within the discipline of International Relations, insights from cognitive psychology and social psychology were introduced in a highly influential book by Robert Jervis showcasing the strong influence of individual decision-makers' perceptions and misperceptions on the outcomes of decision-making.[42] Jervis argued that the way in which decision-makers process information and develop beliefs about other actors can lead to misperceptions and strongly contribute to decision-making errors.[43]

The influence of cognitive factors has been shown to be particularly strong in cases of situational uncertainty, where "the true probability of outcomes cannot be precisely predicted" and

[40] Robert Powell, 'Absolute and Relative Gains in International Relations Theory', *The American Political Science Review* 85, no. 4 (1991): 1303, https://doi.org/10.2307/1963947.
[41] Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (1 January 2017): 58, https://doi.org/10.1162/ISEC_a_00266.
[42] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, New Jersey: Princeton University Press, 1976), 6–9.
[43] Jervis, 10.

where humans have to weigh up different costs of alternative decisions.[44] Indeed, research in evolutionary biology has shown that humans have evolved biases as solutions to decision-making problems in situations where they are faced with incomplete information.[45] According to Tversky and Kahneman, these biases, which can lead to errors of judgement, result from certain heuristic principles that reduce the complexity of assessing probabilities and predicting values.[46] Under conditions of uncertainty, wrote Jervis, "decision-makers often see imaginary dangers." "They are sensitive to threats to their security that critical observers regard as miniscule."[47]

Cognitive and psychological approaches have also sought to explain risk aversion and risk acceptance. Prospect Theory predicts risk aversion in "choices involving sure gains" and risk-seeking in "choices involving sure losses."[48] Rose McDermott, for example, used Prospect Theory to compare the decisions of President Jimmy Carter to exclude the Shah of Iran from the United States in 1979 and to undertake the (failed) hostage rescue mission in Iran in 1980, showing that the first decision was made in the domain of relative gains, whereas the second was a gamble to recoup losses.[49]

The major shortcoming of cognitive approaches is their inability to explain how different decision-makers arrived at the same or similar choices; behavioural traits of human nature are not "fixed" so leaders are likely to vary in their individual dispositions.[50] Cognitive approaches are also less useful in explaining decision-making processes that involve multiple people in groups or bureaucracies.[51] Cyber-related decision-making is particularly likely to involve multiple advisors and policymakers because, as a highly complex and largely virtual domain, it requires a base of technical knowledge and understanding of computer networks and malicious code. State leaders, in their reliance upon experts for technical guidance, are likely to have a comparatively less direct influence on decision-making regarding cyber issues than they would in areas related to the physical domain or more general foreign policy. As we will see in the US chapter, in the case of the 2016 election interference, President Barack Obama considered various response options in close consultation with a group of cyber experts, including then Director of National Intelligence, James Clapper. This meant that although the level of presidential involvement in response decision-making on that occasion was particularly high, the decisions were not mainly the product of Obama's personal characteristics.

---

[44] Dominic D. P. Johnson et al., 'The Evolution of Error: Error Management, Cognitive Constraints, and Adaptive Decision-Making Biases', *Trends in Ecology & Evolution* 28, no. 8 (August 2013): 2, https://doi.org/10.1016/j.tree.2013.05.014.
[45] Johnson et al., 1.
[46] Amos Tversky and Daniel Kahneman, 'Judgment under Uncertainty: Heuristics and Biases', *Science* 185, no. 4157 (27 September 1974): 1124, https://doi.org/10.1126/science.185.4157.1124.
[47] Jervis, *Perception and Misperception in International Politics*, 373.
[48] Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk', *Econometrica* 47, no. 2 (1979): 263, https://doi.org/10.2307/1914185.
[49] Rose McDermott, *Risk-Taking in International Politics: Prospect Theory in American Foreign Policy* (Ann Arbor: University of Michigan Press, 1998), 11.
[50] Dominic D. P. Johnson, *Strategic Instincts: The Adaptive Advantages of Cognitive Biases in International Politics* (Princeton, N.J.; Oxford: Princeton University Press, 2020), 36.
[51] Johnson, 33.

2.2.3 Constructivist approaches

The "neo-utilitarian" theories outlined earlier assume that ideational factors play only a secondary role (if any role at all) in supporting actors' pursuit of their material interests, which are what really matters to states.[52] Constructivism, by contrast, focuses on what materialist approaches omit: the importance of ideas, identity, beliefs, values, and norms in shaping interstate behaviour.[53] In doing so, it also questions the neorealist and neoliberal assumption that state identities are objectively fixed, arguing instead that they are intersubjectively constructed through social processes and interactions.[54] Importantly, constructivists recognise that material factors exist independently of the social world, but they believe that this material reality is given meaning through actors' ideas and beliefs.[55] Thus, how states reacts to the strategic environment is a result of how the political leadership "understand[s] the world and how they interpret the frequently ambiguous lessons of history."[56] One of the main tenets of constructivism is therefore that states are guided in their interactions in the international system by "intersubjective understandings and expectations" – they react differently towards states they consider friends and states they see as enemies.[57] As Alexander Wendt famously put it, "[a]narchy is what states make of it."[58]

Wendt distinguished his constitutive approach from the "causal approach" to the effect of ideas on policy espoused by Judith Goldstein and Robert Keohane (two prominent neoliberal institutionalists).[59] Whereas Goldstein and Keohane saw power and interests as variables separate to ideas and believed that different variables were able to account for outcomes in different contexts, Wendt believed that the material structure and social structure of international relations are *mutually constituted*; in other words, they affect each other.[60] The task of the constructivist is thus to determine "how identities and norms influence the ways in which actors define their interests *in the first place*

---

[52] John Gerard Ruggie, 'What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge', *International Organization* 52, no. 4 (1998): 855.
[53] Ruggie, 879.
[54] Ruggie, 879.
[55] Emanuel Adler, 'Seizing the Middle Ground: Constructivism in World Politics', *European Journal of International Relations* 3, no. 3 (1 September 1997): 332, https://doi.org/10.1177/1354066197003003003; Christoph O. Meyer and Eva Strickmann, 'Solidifying Constructivism: How Material and Ideational Factors Interact in European Defence', *JCMS: Journal of Common Market Studies* 49, no. 1 (2011): 62, https://doi.org/10.1111/j.1468-5965.2011.02129.x; Jeffrey T. Checkel, 'The Constructivist Turn in International Relations Theory', *World Politics* 50, no. 2 (1998): 325; Bastian Giegerich, *European Security and Strategic Culture* (Baden-Baden: Nomos, 2006), 34.
[56] Robert G. Herman, 'Identity, Norms, and National Security', in *The Culture of National Security*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 277.
[57] Alexander Wendt, 'Anarchy Is What States Make of It: The Social Construction of Power Politics', *International Organization* 46, no. 2 (1992): 396–97.
[58] Wendt, 395.
[59] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), 92–95.
[60] Goldstein and Keohane, *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*, 4.

[emphasis added]."[61] This means that the debate between materialists and constructivists is not about the extent to which ideas explain outcomes better than material forces, but rather the extent to which "brute" material forces (for example human nature, the physical environment, and technological artifacts), versus ideas, have effects on the state's perception of power and interests.[62]

Beyond the above core principles, there is significant variation between scholarly approaches within constructivism. These can be divided into third level approaches, second level approaches, and first level approaches. Third level constructivism explores ideas, beliefs, and identities in the international system – that is, ideational factors that are *shared* by states. In focusing on the emergent properties of the interaction between states in the international system, the work of Wendt is an example of such an approach.[63] Other examples are the works of Martha Finnemore and Kathryn Sikkink on norm "life cycles" and how these affect political change in the international system[64] and the work of Nina Tannenwald on the "systemic phenomenon" of the "nuclear taboo," a global normative revulsion against nuclear weapons which has restrained their use.[65]

Specifically in the area of international cybersecurity, Nye proposed a normative taboo against using cyber capabilities on certain types of targets, for example targeting civilian facilities in peacetime.[66] In another constructivist take on cyber issues, Martha Finnemore and Duncan Hollis, having noted the national security importance of developing shared norms of appropriate state behaviour in cyberspace, criticised the tendency of fora like the UNGGE to treat norms as "the fixed products of negotiation, locked in agreements that can settle expectations." Instead, they drew attention to the importance of norm construction and cultivation through processes like socialisation – thus they argued that international cyber norms will evolve over time through repeated interactions among states.[67] The fact that both these works are, in essence, recommendations for norm construction in cyberspace, is a reflection of the fact that shared cyber norms are still at a very early (first or second) stage of development in the norm "life cycle."[68] Because of this, shared cyber norms cannot readily account for state behaviour.

Other third level constructivist approaches place emphasis on shared state identities in accounting for state behaviour. One example of such an approach is Thomas Risse-Kappen's explanation of NATO's formation and its endurance after the Cold War as a result of a liberal collective

---

[61] Peter J. Katzenstein, 'Introduction: Alternative Perspectives on National Security', in *The Culture of National Security*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 30.
[62] Wendt, *Social Theory of International Politics*, 94–96.
[63] Wendt, 145.
[64] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* 52, no. 4 (1998): 888; Martha Finnemore, *National Interests in International Society*, Cornell Studies in Political Economy (Ithaca, NY: Cornell University Press, 2017).
[65] Nina Tannenwald, *The Nuclear Taboo* (Cambridge, UK: Cambridge University Press, 2007).
[66] Nye, 'Deterrence and Dissuasion in Cyberspace', 61.
[67] Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International Law* 110, no. 3 (July 2016): 477, https://doi.org/10.1017/S0002930000016894.
[68] Mazanec quoted in: Nye, 'Deterrence and Dissuasion in Cyberspace', 62.

identity and shared democratic values.[69] Another example is Michael Barnett's work on alliance formation: Barnett argued that common identities and shared western liberal democratic values between the United States and Israel is what forged their alliance.[70] As Chapter 1 already noted, the states under consideration in this thesis were all western liberal democracies – indeed, two were precisely the United States and Israel. Although all three states held shared values, they responded very differently to cyber attacks. Thus, systemic ideational accounts also fail to account for the research puzzle.

Second level approaches prioritise the ideas and beliefs of *countries* and *regimes*. As we will see in the empirical chapters, national ideational differences are crucial to answering our research question. This thesis therefore builds on second level constructivism and argues that the characteristics of a country's culture and historical experience lay the best foundations for explaining the differences in responses (we will therefore return to this point below). First level approaches focus on the ideas and beliefs of *individuals*. An example of a study that adopts such a framework is John G. Stoessinger's investigation into why nations go to war with reference to leaders' personalities and beliefs.[71]

Second level approaches are inspired by Max Weber's assertion that humans are "cultural beings."[72] IR scholars have traced a broad array of policy outcomes to states' internal cultures. Stephen Rosen, for example, argued that the nature of the dominant social structures in a country can affect the amount of military power generated by that country.[73] Elizabeth Kier showed that choices between offensive and defensive military doctrines are explained by policymakers' cultural environments.[74] Second level approaches have also investigated the influence of key historical events on beliefs and values and their impact on subsequent policies of restraint. For example, scholars showed how the Powell Doctrine, employed in the late 1980s and early 1990s most prominently in Operation Desert Storm in Iraq, was a product of the "lessons learned" by the Pentagon from the Vietnam War. It advocated the last-resort application of military force only in support of clearly defined national interests.[75] In Germany, "the habitus of restraint," particularly visible in the diverging opinions between Washington and Berlin on the case for war in Iraq, was shown to have been driven by anxiety and

[69] Thomas Risse-Kappen, 'Collective Identity in a Democratic Community: The Case of NATO', in *The Culture of National Security*, ed. Peter Katzenstein (New York: Columbia University Press, 1996), 378.
[70] Michael N. Barnett, 'Identity and Alliances in the Middle East', in *The Culture of National Security*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 445–47.
[71] John George Stoessinger, *Why Nations Go to War* (Belmont, CA: Thomson/Wadsworth, 2008), 254.
[72] Max Weber, *On the Methodology of the Social Sciences* (Philadelphia, Pennsylvania: The Great Library Collection by R.P. Pryne, 1949), 81.
[73] Stephen Peter Rosen, 'Military Effectiveness: Why Society Matters', *International Security* 19, no. 4 (1995): 6, https://doi.org/10.2307/2539118.
[74] Elizabeth Kier, 'Culture and French Military Doctrine Before World War II', in *The Culture of National Security*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 187.
[75] Jeffrey Record, 'Back to the Weinberger-Powell Doctrine?', *Strategic Studies Quarterly* 1, no. 1 (2007): 79; Alexander Wolf, 'US Interventions Abroad: A Renaissance of the Powell Doctrine?', *Strategic Studies Quarterly* 3, no. 4 (2009): 126.

shame rooted in its experience of the Second World War.[76] In Japan, the country's pacifistic military culture can also be traced back to Japan's role in the same war.[77] The cases of Germany and Japan were also true puzzles for neorealists who had predicted – on the basis of strictly material and systemic considerations – that the two states would seek to acquire nuclear weapons after the change in the structure of the international system at the end of the Cold War.[78]

In taking a sociological perspective to explain national security decisions, this thesis seeks to contribute to the second level constructivist literature on the role of the internal culture of states and ideas in international security.[79] Beck's risk society notion allows us to supplement second level constructivism to provide a full account of variance in responses to cyber threats, which rational, material theories cannot do. Concretely, the risk framework allows us to integrate the tenets and insights of second level constructivism with the realities and characteristics of cyberspace to explain variation in state responses to cyber attacks. It does this by elucidating the interaction between technological progress and culture to produce societal risk aversion, which, as this thesis will show, manifests particularly in cybersecurity related decision-making. Consistent with constructivist theoretical assumptions, the thesis will show that societal risk aversion or risk acceptance shaped different actors' perceptions of how best to pursue their interests in face of perceived external risks or threats. Consequently, although the cyber operational environment created constant pressures and constraints across the three case studies, different states reacted to these pressures and constraints in starkly different ways.

An oft-repeated criticism of studies privileging culture and ideas is that the concepts are difficult to define and operationalise, and therefore have limited utility for formulating testable theories.[80] As the later discussion of the risk society literature will show, Ulrich Beck's concept of the risk society suffers from similar difficulties. In particular, Beck's theory only explicitly deals with highly industrialised western societies and does not consider the perceptions and behaviour of societies that have not yet reached the same level of modernisation and technological dependence as the west, or that have different cultural or historical predispositions (this is merely implied). Moreover, Beck and

[76] Corneliu Bjola and Markus Kornprobst, 'Security Communities and the Habitus of Restraint: Germany and the United States on Iraq', *Review of International Studies* 33, no. 2 (April 2007): 286–87, https://doi.org/10.1017/S0260210507007516.
[77] Thomas U. Berger, 'Norms, Identity, and National Security in Germany and Japan', in *The Culture of National Security* (New York: Columbia University Press, 1996), 317–56.
[78] John S. Duffield et al., 'Isms and Schisms: Culturalism versus Realism in Security Studies', *International Security* 24, no. 1 (1999): 159.
[79] See for example: Peter J. Katzenstein, ed., *The Culture of National Security* (New York: Columbia University Press, 1996); Alastair Iain Johnston, 'Thinking about Strategic Culture', *International Security* 19, no. 4 (1995): 41, https://doi.org/10.2307/2539119; Rosen, 'Military Effectiveness', 24; Duffield et al., 'Isms and Schisms'; Tannenwald, *The Nuclear Taboo*.
[80] Some thinkers also believe that cultural explanations are incompatible with rationality. Yet, as Alastair Iain Johnston explained, this is not necessarily true. It is instead more accurate to see culture as simplifying reality, defining actors' ranked preferences or otherwise narrowing their options. See: Johnston, 'Thinking about Strategic Culture', 34; Michael C. Desch, 'Culture Clash: Assessing the Importance of Ideas in Security Studies', *International Security* 23, no. 1 (1 July 1998): 151, https://doi.org/10.1162/isec.23.1.141.

the sociologists provided almost no indication of which cultural values specifically contributed to the emergence of western risk societies. To address the first issue, one of the contributions of this thesis to the risk literature is to develop, based on Beck's work, a risk spectrum, whose purpose is to establish the observable behavioural implications of states high on the risk spectrum (risk societies) and states low on the risk spectrum (threat societies), which in turn will enable cross-case measurement and comparison. To remedy the second issue, this thesis refers to the IR literature on strategic culture to draw out the beliefs and values that have influenced how different societies engage in security related decision-making.

Having outlined the main theories of International Relations and positioned the theoretical framework of this thesis within them, the remainder of this chapter will examine the theory of the risk society in greater depth and develop the risk framework, which in later chapters will guide the empirical investigation of the thesis's research question.

2.3 The risk framework

The central argument of this thesis, which builds on the theory of the risk society, is that states that have a strong desire for risk avoidance and minimisation – states that this thesis labels risk societies – will perceive the uncertainties inherent in cyberspace as an obstacle to issuing meaningful punishment, resulting in weak responses to foreign cyber attacks. Conversely, states that are risk acceptant/ threat sensitive – states that this thesis labels threat societies – will be less affected by these uncertainties and focus their attention on the historical and ideological threat of their main adversary, resulting in meaningful responses. States that are culturally risk acceptant/ threat sensitive but embedded in a risk community (which they perceive as providing the ultimate guarantee of their survival) will defer to the risk sensitivities of that community, resulting in the lack of meaningful punishment.

The value of the risk society theory from Sociology in relation to his argument can be summarised in two main points. First, it elucidates the mechanism which gave emergence to the palpable sense of fear and anxiety within highly industrialised and technologically dependent western societies: reflexive modernity. Under conditions of reflexive modernity, the theory holds, societies will be consumed by a focus on risks. Second, in relation to this diagnosis, it inspired a definition of risk which focuses on worst-case scenarios that are unwanted side effects of a state's own actions, but highlighted that risk is socially and culturally constructed, meaning that not all states will perceive risks in the same way. A third contribution is provided by the "war as risk management" literature, which extended the risk society theory and predicted that risk-sensitive states are more likely to engage in preventive action rather than reactive approaches.

To examine these contributions in greater detail, this section will first introduce the main elements of the risk society theory. It will then discuss the definition of risk central to the main argument

of this thesis and extend the theory in developing the concept of the threat society. The final part will discuss scholarly challenges to the risk society thesis.

2.3.1 The origins of the risk framework in Sociology

The idea of the "risk society" first originated from German sociologist Ulrich Beck, offering a compelling sociological explanation for what Beck saw as the west's move away from a "narrative of modernisation and progress," which had characterised the industrial era, and into an age of "reflexive modernity."[81] This reflexive modernity is important for our purposes because it marks the starting point of the explanation of how some societies became particularly sensitive to risks. According to Beck, the processes of modernisation, meaning technological, scientific, and industrial development, were producing a series of unanticipated and unintended risks and hazards that states and societies were struggling to contend with. It is not that Beck thought that everyday life had become more dangerous, rather, he observed that risks had become "de-bounded" in the sense of no longer being confined to nation-state boundaries, no longer being constrained temporally (as they had a long latency period), and no longer being the attributable to one source (they were a result of a constellation of factors and the combined effects of actions of many individuals).[82] His early work particularly emphasised ecological crises such as climate change, nuclear waste, and environmental pollution. He argued that in the modern era, the "darker side" of industrialisation and globalisation had led to the emergence of "risk societies": societies preoccupied chiefly with preventing and minimising the uncertain hazards created by these processes.[83] According to Beck, "the speeding up of modernization … produced a gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities that we are creating."[84] Rather than being preoccupied with the distribution of power and wealth, as was the case in industrial societies, risk societies are especially concerned with risk management.[85]

The concept of reflexive modernity in the work of Beck, Anthony Giddens, and Scott Lash, signifies a new stage of development that modern societies have entered into, in which "progress turns into self-destruction" and "one kind of modernization undercuts and changes another."[86] Within modern western civilization particularly, explained Giddens, an *awareness* of the negative side effects of scientific and technological advances forced these societies to confront a "diversity of possible futures,"

---

[81] Beck, *Risk Society*; Adam Tooze, 'The Sociologist Who Could Save Us From Coronavirus', Foreign Policy, 1 August 2020, https://foreignpolicy.com/2020/08/01/the-sociologist-who-could-save-us-from-coronavirus/.
[82] Ulrich Beck, 'The Terrorist Threat: World Risk Society Revisited', *Theory, Culture & Society* 19, no. 4 (1 August 2002): 41, https://doi.org/10.1177/0263276402019004003.
[83] Michael J. Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', *Cooperation and Conflict* 43, no. 1 (2008): 59–60, https://doi.org/10.1177/0010836707086737.
[84] Beck, 'The Terrorist Threat', 41.
[85] Jeffrey Wimmer and Thorsten Quandt, 'Living in the Risk Society: An Interview with Ulrich Beck', *Journalism Studies* 7, no. 2 (1 April 2006): 337, https://doi.org/10.1080/14616700600645461.
[86] Ulrich Beck, Anthony Giddens, and Scott Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity in association with Blackwell, 1994), 2.

leaving them feeling perpetually insecure.[87] Societies living under conditions of reflexive modernity see technologies as generating consequences in their application whose implications are "unforeseen, unintended or unknowable."[88] In other words, risk societies are "reflexive" in the sense that they have to contend with risks that are a by-product of their own actions and technological advancement.[89] The increased societal awareness of these negative side effects creates in risk societies a widespread anxiety about the uncertainty of future scenarios.[90]

In contrast to Cold War-era threats, which were typically well-defined and elicited a clear reaction (for example the number of nuclear missiles possessed by the Soviet Union[91]), the uncertainty of present security challenges and the consequent inability to make decisions based on calculations of causes and effects confounds societies with a low tolerance for risk.[92] Risk-conscious policymakers consider policy options in terms of probabilistic future scenarios: what catastrophic attack *might* terrorists be planning, which regimes *may* be developing nuclear capabilities, and what is the likelihood that the two *might* collude, for example.[93] Therefore, in contrast to the direct, linear, and "instrumental" rationality of the past, the current era for risk societies is characterised by a "reflexive rationality," which is concerned with continuously trying to identify potential risk and intervene in time to avert a range of undesirable consequences that may or may not materialise.[94]

Risk, according to Beck, is the primary force guiding decision-making in reflexive societies – it leads to "international politics as risk minimization."[95] The major motivating force in Beck's risk society is safety and security; accordingly, risk societies engage in risk management to address anxieties and fears about future threats.[96] Indeed, the mitigation of risk becomes in risk societies the "central element of politics and public policy."[97] However, risk management also comes at a price: a paradox the sociologists observed was that every risk mitigation strategy in itself can create new uncertainties and unintended side effects that sometimes impede risk mitigation in other areas, possibly leading to an even greater sense of perceived insecurity.[98]

---

[87] Giddens, 'Risk Society: The Context of British Politics', 23; Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', 60.
[88] Darryl S. L. Jarvis, 'Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis', *Global Society* 21, no. 1 (2007): 28, https://doi.org/10.1080/13600820601116468.
[89] Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', 60.
[90] Beck, *World Risk Society*, 143.
[91] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London ; New York: Routledge, 2010), 1; Beck, *World Risk Society*, 61.
[92] Heng, *War as Risk Management*, 2006, 52; Beck, *World Risk Society*, 61.
[93] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 2010, 1.
[94] Heng, *War as Risk Management*, 2006, 13; Shahar Hameiri and Florian P. Kühn, 'Introduction: Risk, Risk Management and International Relations', *International Relations* 25, no. 3 (2011): 276, https://doi.org/10.1177/0047117811415479.
[95] Wimmer and Quandt, 'Living in the Risk Society: An Interview with Ulrich Beck', 342.
[96] Heng, *War as Risk Management*, 2006, 34.
[97] Ronald J. Deibert and Rafal Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology* 4, no. 1 (2010): 18, https://doi.org/10.1111/j.1749-5687.2009.00088.x.
[98] Deibert and Rohozinski, 18.

The emergence of transnational, unconventional, and temporally unconstrained security risks in the late 1980s wasn't, however, the only factor that contributed to the development of risk societies. Equally important was the collapse of the Soviet Union, which left western countries without a geopolitical primary adversary or state-based threat. The concern in north America and western Europe with new risks was therefore what filled the void left by this seismic event in world politics.[99] Indeed, according to Beck, the new risk society was not "born in pain" through "growing poverty," but rather it was "growing wealth and the loss of an Eastern rival" that "produce[d] an axial change in the types of problems, the scope of relevance and the quality of the political."[100] As this thesis will argue in Chapter 6, these very same dynamics co-produced (alongside cultural factors) a change in NATO's identity from a "security community" to a "risk community."[101] In this sense, referring to the constructivist approaches in IR, the fall of the Soviet Union is a good example of a material change in systemic conditions that "create[d] spac[e] for new ideas to emerge" – ideas about the unpredictability of the new global security environment.[102] The shift in the international security landscape did not, however, affect all states in the same way; as this thesis will also argue, Estonia, despite the fall of the Soviet Union and its own accession into NATO, as a result of its traumatic history of Soviet occupation, retained its national security focus on the existential threat posed by Russia, even at a time when western relations with Moscow were at a historical high point. This is because, as we will discuss in the next section, risk is socially constructed and perceived; it is not the result merely of material threats and circumstances. The differing interpretations of the fall of the Soviet Union highlight the complex interplay of material and ideational factors and their co-constitution.[103]

2.3.2 Defining risk

Beck defined risk as "the modern approach to foreseeing and controlling the future consequences of human action [and] the various unintended consequences of radicalised modernisation."[104] Crucially, however, "risk is inherently affected by politics and the culture of each state"; social, historical and cultural factors came into play when people decide what they consider to be risks and how to address them.[105] Thus, Beck and Giddens took the position of "critical realists",

[99] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 2010, 6.
[100] Ulrich Beck, Anthony Giddens, and Scott Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity Press, 1994), 3.
[101] Christopher Coker, *Globalisation and Insecurity in the Twenty-First Century: NATO and the Management of Risk*, Adelphi Papers ; No. 345 (Oxford and New York: Oxford University Press for the International Institute for Strategic Studies, 2002).
[102] Meyer and Strickmann, 'Solidifying Constructivism', 68.
[103] Meyer and Strickmann, 68.
[104] Beck, *World Risk Society*, 4.
[105] Nathan G. Garrett, 'NATO, Security and Risk Management: From Kosovo to Kandahar, by Williams, M. J.', *The Journal of Slavic Military Studies* 23, no. 3 (3 September 2010): 525, https://doi.org/10.1080/13518046.2010.503171; William Clapton, 'Risk in International Relations', *International Relations* 25, no. 3 (2011): 282–83, https://doi.org/10.1177/0047117811415480.

adopting a "realist ontology" and a "constructivist epistemology."[106] Like constructivist approaches in IR, they understood risks to be rooted in material realities, but believed that the way in which societies and policymakers identify risks is dependent on constructivist interpretations rather than "scientific or objective quantification."[107] Explaining this point further, Douglas and Wildavski wrote, "we choose the risks in the same package as we choose our social institutions. Since an individual cannot look in all directions at once, social life demands an organisation of bias."[108] This bias is "wired" by cultural, societal, and historical factors.[109] Because the perception of risks is subjective and culturally constructed, "some societies take more risks than others."[110] In sum, the extent to which a society is a risk society depends on the interplay of material factors (for example, the distribution of material capabilities in the international system) as well as ideational factors, like culture and lessons from history, which shape perceptions of material reality.

Security studies scholars from within the "war as risk management" literature have, however, noted the difficulty in operationalising Beck's concept of risk.[111] Yee-Kuang Heng observed that "Beck appeared more intent on understanding [the] implications and political significance [of risk] than defining the concept."[112] Coker noted that "risk" in English conveys a wide range of "invented meanings," much like the German term "Sicherheit," which was used in Beck's original work.[113] Building on Beck's definition, Heng observed that "risk is associated with the possibility that an adverse state of reality may occur as a result of natural events or human (in)action." Relevant in the context of policymaking, the consequences of this (in)action can theoretically be altered by changing the initiating activity or lessening its impact. "Risk thinking" is therefore characterised by anticipating events and "assessing present options in terms of the future."[114] For the purposes of this thesis, drawing from Heng's definition, risks are understood to be diverse, potential, and uncertain scenarios, usually

---

[106] Hameiri and Kühn, 'Introduction', 276.

[107] Hameiri and Kühn, 276; Yee-Kuang Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', *Contemporary Security Policy* 39, no. 4 (2 October 2018): 547, https://doi.org/10.1080/13523260.2018.1494670; Karen Lund Petersen, 'Risk Analysis – A Field within Security Studies?', *European Journal of International Relations* 18, no. 4 (2012): 704, https://doi.org/10.1177/1354066111409770; Clapton, 'Risk in International Relations', 282–83. The sociological approach to risk is different to that of Copenhagen School scholars in International Relations, who take an entirely constructivist/ critical theoretical stance, arguing that security should be seen as a "speech act" where issues are entirely socially constructed as risks without any material basis. For an example of a strictly constructivist approach to risk see: Ole Wæver, 'Securitization and Desecuritization', in *On Security*, ed. Ronnie Lipschutz (New York: Columbia University Press, 1995), 46–86.

[108] Mary Douglas and Aaron B. Wildavsky, *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers* (Berkeley: University of California Press, 1982), 23.

[109] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 2010, 23.

[110] Christopher Coker, 'Between Iraq and a Hard Place', *The RUSI Journal* 151, no. 5 (1 October 2006): 18, https://doi.org/10.1080/03071840608522868.

[111] Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', 61; Yee-Kuang Heng, 'War as Risk Management' (London, London School of Economics and Political Science, 2003), http://etheses.lse.ac.uk/1714/1/U183174.pdf.

[112] Heng, *War as Risk Management*, 2006, 44.

[113] Coker, *War in an Age of Risk*, 64.

Rasmussen, *The Risk Society at War*, 3; Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', 2 October 2018, 547.

connected to technological progress, and often an unintended result of a prior action or decision or a series of actions taken by a state.

To further clarify the definition of risk, it is helpful to compare it to the concept of threat, a distinction which Chapter 1 already touched upon. While both concepts hinge on the perception of an independently existing material basis, the major difference is that the idea of a threat is "indelibly linked to the idea of another actor"; an example of such an actor was the Soviet Union during the Cold War.[115] Conversely, risk can be perceived "independently of an identifiable actor."[116] Unlike threats, risks are perceived to defy assessment in terms of clear "intentions and capabilities."[117] Risks therefore necessarily imply uncertainty.[118]

2.3.3 The threat society: a refinement of risk society thinking

This thesis introduces the concept of the "threat society" as an important refinement of risk society thinking. It uses the difference between threats and risks to distinguish between how different societies view the security environment; in doing this, the thesis is also able to place states on a spectrum of risk. States high on the risk spectrum, risk societies,[119] will usually lack a single principal adversary – their major preoccupation instead will be more diverse dangers whose occurrence they see as uncertain. As a result of cultural biases and their historical experience, risk societies will, under conditions of uncertainty, have a tendency to imagine multiple worst-case scenarios. They will see risk as "an unacceptable danger and negative outcom[e] to be avoided."[120] Conversely, states low on the risk spectrum, threat societies, also as a result of their own culture and history, are unlikely to regard uncertainty and risks as *unacceptable*; instead, they will be more focused on dangers that, again, through a cultural and historical lens, they perceive as being traced to one single, imminent, and clearly defined existential *threat.* Although the assessment of threats might be seen to lend itself to more objective analysis through quantification (for example, estimating the number of ballistic missiles in a country's possession), the *meaning* ascribed to the outcome of such a quantitative exercise will depend heavily on ideas and beliefs (for example, beliefs that the country holds about the owner of those ballistic missiles). What this means is that, while material realities can enhance or decrease a state's view of the security landscape as dominated by risks or one particular threat, in the end, it is beliefs and ideas that ascribe meaning to those risks and that threat.

---

[115] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 2010, 18.
[116] Williams, 18.
[117] Williams, 19.
[118] Williams, 18–19.
[119] As Chapter 1 already noted, a group of risk societies can also form a "risk community." NATO is an example of such a risk community, which will be discussed in detail in Chapter 6.
[120] Heng, *War as Risk Management*, 2006, 44–45.

Although the empirical chapters of this thesis refer to risk societies and threat societies, in reality states' dispositions towards risk are unlikely to fall neatly into binary categories; thus the concept of a spectrum more accurately reflects this more nuanced empirical reality. As we discussed, this thesis places risk societies high on the spectrum and threat societies low on the risk spectrum. Mid-spectrum societies are those combining the characteristics of risk societies and threat societies; these are likely to be caught between a developing societal awareness of the negative side effects of modernisation, on the one hand, and the fear of a concrete state-based threat, on the other. It should be noted that neither the Sociology literature nor the war as risk management literature examines threat societies or mid-spectrum societies, offering instead the distinction between a threat-based rationality and a risk-based rationality as the only reference point.[121] The table below elucidates the key characteristics of risk societies, mid-spectrum societies, and threat societies.

Table 4: The risk spectrum

Risk profile	Societal characteristics
Risk society	• Reflexive: especially concerned with the unintended consequences and negative side effects of the society's own technological progress and modernisation. • Preoccupied with risks, meaning diverse, potential, uncertain (frequently worst-case) scenarios, usually connected to technological progress, that are often an unintended consequence of an action or decision. This translates into careful considerations of the potential side effects and blowback from the state's own activity. Often involves the careful weighing up of costs and benefits of any action with reference to potential future scenarios. • Proactive in the application of preventive measures and/or paralysed decision-making in reaction to an incident: likely to either engage in preventive measures to manage risks and likely to experience paralysis in the aftermath of an incident (as opposed to taking a strong reactive approach).[122]

[121] Heng, 49.

[122] As Beck wrote: "To the extent that risks become the all-embracing background for perceiving the world, the alarm they provoke creates an atmosphere of powerlessness and paralysis." See: Beck, *World Risk Society*, 138. And: "With risks, avoidance imperatives dominate. Someone who depicts the world as risk will ultimately become incapable of action. The salient point here is that the expansion and heightening of the intention of control ultimately end up producing the opposite." See: Ulrich Beck, 'The Reinvention of Politics: Towards a

Mid-spectrum society	• Still subscribes to the "narrative of modernization and progress," but this is punctuated by periods of awareness of negative side effects of industrialisation. [123] • Increasingly concerned with risks, but not yet displaying routine reasoning and decision-making with reference to diverse, worst-case scenarios stemming from unintended effects of the state's own actions (second or third order effects). • Maintains its focus on well-defined threats, leading to the continuing employment of reactive strategies, usually combined with preventive measures.
Threat society	• Exhibits a willingness to accept risks: the potential for unintended consequences does not diminish the resolve to act. Unintended consequences of the state's own actions might not even appear in the decision calculus. • Seeks self-reliance (often under a military doctrine of total defence[124]). • Preoccupied with what it perceives as a well-defined, imminent existential threat, stemming from one particular state actor. • Reactive: prefers response over preventive measures (although may also engage in preventive measures as an addition to reactive strategies) and reacts strongly and

Theory of Reflexive Modernization', in *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, ed. Ulrich Beck, Anthony Giddens, and Scott Lash (Cambridge: Polity Press, 1994), 9.

[123] As the empirical chapters will reveal, none of the countries considered in the case studies of this thesis fell in the middle of the risk spectrum. For the purposes of illustration here, a country that might be considered to be in such a position is China. On the one hand, risks like climate change, pollution, and pandemics on occasion undercut the Chinese narrative of progress, leading to an awareness of the negative side effects of progress (reflexivity) but, on the other, China's tensions with its neighbours over the South China Sea and other disputed territories keep attention focused on state-based threats to territorial sovereignty. Chinese historical memory of Japan's invasion in 1944 likely contributes to such a focus. The Chinese case is, however, highly complex, not least because of the firm hold over society of the Chinese Communist Party, which quickly suppresses any internal questioning of what Adam Tooze calls "the modern epic of the China dream." The extent to which China becomes more sensitive to risks in the near future will likely depend significantly on domestic political developments and their interplay with cultural and historical factors. (See: Tooze, 'The Sociologist Who Could Save Us From Coronavirus'.)

[124] Total defence is defined as "a security approach involving all of society, under the democratic control of political authorities, and through an institutional collaboration between these authorities, the armed forces, civil administrations, the private sector and the public. It aims to deter a potential enemy by increasing the cost of an attack and reducing its chances of success." See: Joelle Garriaud Maylam, 'Committee on the Civil Dimension of Security: Enhancing the Resilience of Allied Societies Through Civil Preparedness' (Brussels, Belgium: NATO Parliamentary Assembly, 3 March 2021), 2.

	decisively. Favourable to deterrence by punishment.

Adopting Beck and Giddens' critical realist approach, the framework in this chapter suggests that the properties of the cyber domain and the uncertainty they introduce into policymaking will be interpreted differently depending on where a state falls on the risk spectrum, which in turn will depend on a constellation of historical, societal, and cultural factors (and although the relevant empirical chapters will position the country case studies within a historical and cultural context and explain the emergence of either the risk society or the threat society in each case, it should be noted that an extensive examination of the sources of particular societal beliefs is beyond the scope of the thesis). In cases where states hold a strong desire for risk avoidance and minimisation, the framework predicts that the uncertainty inherent in the cyber strategic environment will play a defining role in their response calculus, leading to greater restraint in individual responses and an increased focus instead on practices of risk management as a general approach to cyber issues. In cases where states are threat societies, they will pay less attention to the risks of the operational environment due to their focus on a perceived existential threat and will engage in meaningful punishment of foreign cyber attacks.

Finally, it is important to note that employing a risk sensitive calculus does not necessarily translate into inaction or general restraint. The crucial point, rather, is that risk frames debates in terms of anticipating future adverse events that might arise as an unintended effect of one's own actions, so as to avoid worst-case scenarios.[125] Depending on how future events are anticipated, risk management can result in policy paralysis or in taking a *highly proactive* defensive stance and engaging in preventive campaigns to manage future risk (see Table 3).[126] The "war as risk management" literature particularly highlighted the tendency of risk societies to engage in "precautionary risk management strategies" as a response to scenarios they consider intolerable and difficult to predict.[127] The next chapter will examine how the technical features of the cyber domain are likely to lead states to adopt risk management practices, including preventive action. Thus, while a risk society is likely to be more restrained than a threat society in the administration of punishing responses to *individual* cyber attacks, it may be equally active in the application of preventive measures in an effort to reduce perceived risk (as we will see in Chapter 3, in the context of the War on Terror, such preventive measures paradoxically resulted in increased risk).

[125] Yee-Kuang Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', *Contemporary Security Policy* 39, no. 4 (2 October 2018): 547, https://doi.org/10.1080/13523260.2018.1494670.
[126] An example of such a forceful pre-emptive campaign was President Bush's 2003 regime change campaign in Iraq. For an elaboration of the Iraq war as a risk management campaign see: Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006).
[127] Heng, *War as Risk Management*, 2006, 57.

2.3.4 Challenges to the risk society thesis

The criticisms of the risk society thesis can be grouped into two main themes. The first questions Beck's diagnosis of the true extent of risks in post-industrial modernity. Bryan Turner, for example, argued that previous historical eras witnessed similar risks to the ones societies contend with today – pandemics and environmental catastrophes for example – and similarly led to "profound uncertainties about life, which occasionally overwhelmed previous civilizations."[128] Darryl Jarvis also took issue with Beck's "philosophy of fatalism," pointing out that since the end of the Cold War, nuclear arsenals have been reduced and the prospect of nuclear weapons accidents has diminished.[129] However, while the empirical record may indeed raise questions about the level of real danger present in the post-Cold War era, it is important to note that Beck highlighted the importance of the *perception* of risk and the increased sensitivity to it in certain societies, rather than its objective material existence. Indeed, Jarvis himself went on to concede that "[i]t is, perhaps, not so much a question about whether there are more risks but how we perceive them and the adequacy of their management, compensation and mitigation."[130] The risks that Beck pinpointed were rooted in material reality – transnational terrorism, for example, presented a real material danger – but Beck's contribution was to show that western societies, associating the growth in the risk of terrorism with their own technical progress, reacted to that danger with alarmism and intense anxiety, which reduced trust in other citizens and states (therefore actually multiplying risks): "[t]hus the terrorist threat has made everyone into a disaster movie scriptwriter, now condemned to imagine the effects of a home-made atomic bomb assembled with the help of gene or nanotechnology; or the collapse of global computer networks by the introduction of squads of viruses … ."[131] As this thesis will seek to show, differences in risk and threat perception are key to understanding variations in states' reactions to material conditions.

A second critique of Beck's theory posits that his "critical realist" approach creates internal inconsistencies. By referring to the "world risk society" – which in fact is the title of one of his key works – Beck seemed to imply that perceptions of risk can be generalised.[132] Such portrayals seem to directly contradict the point that perceptions of risk are culturally and socially informed.[133] Moreover, as we already discussed, the risk society literature provides few, if any, clues as to what happens outside highly industrialised western societies. Even in his treatment of western societies, Beck failed to capture

---

[128] Turner quoted in: Anthony Elliott, 'Beck's Sociology of Risk: A Critical Assessment', *Sociology* 36, no. 2 (1 May 2002): 300, https://doi.org/10.1177/0038038502036002004.
[129] Jarvis, 'Risk, Globalisation and the State', 43.
[130] Jarvis, 46.
[131] Beck, 'The Terrorist Threat', 44–46.
[132] Gabe Mythen, 'Reappraising the Risk Society Thesis: Telescopic Sight or Myopic Vision?', *Current Sociology* 55, no. 6 (1 November 2007): 800, https://doi.org/10.1177/0011392107081986; John Tulloch and Deborah Lupton, *Risk and Everyday Life* (London: Sage, 2003); Iain Wilkinson, *Anxiety in a Risk Society* (London: Routledge, 2001).
[133] Mythen, 'Reappraising the Risk Society Thesis', 800.

differences in risk sensitivity among western nations. These observations have led critics to charge that Beck "affords insufficient attention to the rooted everyday contexts in which risks are routinely interpreted and negotiated."[134] Indeed, the risk sociologists' penchant for "grand theorizing" left them open to the charge that they oversimplified empirical realities.[135] To gage the changing and dynamic nature of the concept of risk, and thus avoid the dangers of generalisation, Deborah Lupton advised researchers following Beck's risk society thesis to investigate different social groups' understandings of risk, with particular attention to variation between countries.[136] In investigating conceptualisations of risk and threat in three country case studies and developing the concept of the threat society, this thesis endeavours to implement Lupton's advice.

2.4 Conclusion

This chapter began with a discussion of how different theoretical approaches from International Relations might consider the research question of this thesis and pointed out their shortcomings. In the case of neorealism, the theory struggles to account for state responses to cyber attacks due to its difficulty in accommodating hostile operations involving intangible weapons whose effects have not reached the level of traditional armed conflict. Neoliberal institutionalism, for its part, also finds it difficult to account for differences in states' responses to cyber attacks when there is a lack of regimes and international institutions regulating cyber conflict. Complex interdependence theory fails to account for differences in response between the United States and Estonia, on the one hand, and Israel, on the other, given that all three states are equally deeply embedded in networks of co-dependence. Finally, cognitive and psychological approaches focusing on a single leader cannot explain why different government administrations arrived at similar decisions and cannot explain decisions that were made in consultation with groups of experts. More promising were constructivist approaches, which, the chapter discussed, the theory of the risk society broadly falls under – particularly second level approaches focusing on the cultural ideas and beliefs that prevail in domestic societies.

After positioning the guiding theory of this thesis within the IR literature, the chapter turned to discussing the risk society theory itself. Originating in Sociology, the major strengths of the theory are its diagnosis of western societies' entry into a stage of reflexive modernity, where societies have become anxiously aware of the negative side effects of technological progress, and its observation that these societies have become intensely preoccupied with risks – defined as diverse and highly uncertain future scenarios resulting from present actions. Two of the three empirical chapters of the thesis will seek to investigate whether such concerns in a known risk society and a risk community can also account for

[134] Mythen, 801.
[135] Deborah Lupton, 'Sociology and Risk', in *Beyond the Risk Society: Critical Reflections on Risk and Human Security*, ed. Gabe Mythen and Sandra Walklate (Maidenhead, Berkshire: Open University Press, 2006), 21.
[136] Lupton, 21.

the lack of meaningful responses to cyber attacks. One weakness that this chapter identified within the theory of the risk society was its lack of attention to societies that do not exhibit reflexivity. Thus, the chapter developed the risk spectrum and, on the basis of the existing risk literature's distinction between risks and threats, elaborated a set of features that were characteristic of societies high on the risk spectrum, mid-spectrum, and at the low end of the spectrum. The addition of the concept of the threat society to signify a society low on the risk spectrum represents an important addition to Beck's theory. By developing this concept, the thesis is able to determine whether risk acceptance and a society's intense preoccupation with a single, well-defined external threat can account for a state's willingness to respond meaningfully to cyber attacks.

The next chapter will relate the features of the cyber domain to the concepts discussed as part of the risk framework. It will seek to show that these features play particularly to the concerns of societies high on the risk spectrum and therefore intensify the risk lens through which they approach national security decisions.

Chapter 3
The Risk Society and Threat Society in the Cyber Domain: Reactions to Operational Uncertainty

3.1 Introduction

Having reviewed the International Relations literature and discussed the risk society theory, we now turn to examining how risk societies and threat societies are likely to perceive and interact with the cyber operational environment.[1]

In the cyber domain, the operational characteristics of the domain create uncertainty among security actors. While threat societies are not expected to see this uncertainty in terms of unacceptable risks that would impede their application of meaningful responses to cyber attacks, risk societies are likely to perceive the operational environment in terms of creating unacceptable risk. In other words, for states culturally and historically conditioned to avoid risk, the operational characteristics of the cyber domain and their consequences in terms of creating uncertainty will pose an obstacle to the application of meaningful responses. By discussing the features of the operational environment that are likely to intensify, by introducing greater uncertainty, a "risk-based system of evaluation and decision-making,"[2] the interpretive framework presented below will help organise and make sense of the empirical case studies in ensuing chapters.

The chapter will start by discussing the sources of operational uncertainty in the cyber domain: cyberspace as a "complex adaptive" system and the ease of proliferation of cyber capabilities. Having done so, it will explain how these operational characteristics contribute to the attribution problem and the potential for unintended effects in cyberspace and show how these two issues complicate the application of meaningful responses by risk societies. Next, the chapter will discuss three risk management practices – preventive action, increasing resilience, and consequence management – and will posit that for risk societies, these three practices will be a central means through which they address the uncertainties of the cyber domain. The final section will seek to show that threat societies, due to their cultural risk acceptance and focus on an existential threat, will not perceive the operational characteristics of the cyber domain and their attendant risks as obstacles to meaningful punishment.

---

[1] Large parts of this chapter were published in: Monica Kaminska, 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks', *Journal of Cybersecurity* 7, no. 1 (9 March 2021), https://doi.org/10.1093/cybsec/tyab008.

[2] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London ; New York: Routledge, 2010), 20.

3.2 Sources of operational uncertainty in the cyber domain

There are two main characteristics of the cyber operational environment that create uncertainties with policy consequences for risk societies: the nature of cyberspace as a "complex adaptive" system and the ease of proliferation of cyber capabilities among offensive actors. This section will explain that these characteristics are sources of uncertainty because they create an unpredictable environment populated by a diverse set of actors and agendas.

3.2.1 Operational characteristic 1: cyberspace as a "complex adaptive" system

As operational environments go, cyberspace is a highly complex system, which can evolve in unpredictable ways.[3] The ways in which a society adopts and relies on the system are also complex, creating compounding layers of complexity.

The US Army visualises cyberspace as comprising three layers: the physical, logical, and social layers, which in turn have five components: geographic space, physical network, logical network, persona, and cyber persona.[4] The physical layer includes the physical location of the network's parts as well as all its hardware and infrastructure; the logical layer, software and lines of code that form connections between the hardware; and the social layer, the people actually on the network and their cyber personas (such as an IP address or email address), which can be multiple.[5] In addition to the Internet of networked computers, there are also intranets, cellular technologies, fibre optic cables, and space-based communications.[6] Complicating things further, as this intricate web of interconnections expanded during the Internet's development, network designers prioritised the convenience of connectivity over the necessity for security against computer-born threats.[7]

Charles Perrow, in his seminal work on "normal accidents", pointed out that complex systems have the following characteristics: unfamiliar or unintended feedback loops, many control parameters with potential interactions, indirect or inferential information sources, and operators' limited understanding of certain processes.[8] In a complex system, small differences in initial conditions can

---

[3] Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge, UK: Cambridge University Press, 2016), 115; Jr Joseph S. Nye, 'From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?', *Bulletin of the Atomic Scientists* 69, no. 5 (2013): 8–9, https://doi.org/10.1177/0096340213501338.
[4] United States Army, 'Cyberspace Operations Concept Capability Plan 2016-2028' (Department of the Army, United States of America, 22 February 2010), 8, https://fas.org/irp/doddir/army/pam525-7-8.pdf.
[5] United States Army, 9; Dave Clemente, *Cyber Security and Global Interdependence What Is Critical?* (London: Chatham House, 2013), 5, http://www.chathamhouse.org/publications/papers/view/189645.
[6] Joseph S. Nye, 'From Bombs to Bytes', 8–9.
[7] Clemente, *Cyber Security and Global Interdependence What Is Critical?*, 6; D. Clark, 'The Design Philosophy of the DARPA Internet Protocols', *ACM SIGCOMM Computer Communication Review* 18, no. 4 (1 August 1988): 106–14, https://doi.org/10.1145/52325.52336.
[8] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, Inc., Publishers, 1984), 86.

produce large changes in patterns of behaviour and unexpected strategic outcomes.[9] The interaction of these processes also has an enormous impact on the potential for system accidents and failure.[10] While especially acute in the cyber context, the problem of complexity is not exclusive to it. Indeed, Perrow famously argued that normal accidents are inevitable in any complex system due to "the way failures interact and the way the system is tied together."[11]

Other scholars have gone further: they have characterised the cyber domain as a complex *adaptive* system.[12] That is, in addition to the above characteristics, the system generates new knowledge that has causal properties of its own, which results in the adaptive behaviour of the system itself. Consequently, the system evolves in ways that the system's designers themselves did not envisage.[13] Complex adaptive systems therefore tend to exhibit "chaotic behaviour,"[14] which complicates enormously the task of predicting their failure rates.[15]

Then there is the issue of interconnections among critical infrastructures. Much like a central nervous system, cyberspace runs through these infrastructures, including communications, emergency services, government, food, water, health, transport, finance, and energy, allowing them to communicate and function.[16] By implication, unless a system is "air-gapped," a failure in one infrastructure has the potential to cascade into others, significantly raising the probability of unanticipated consequences.[17] More specifically, the vast majority of critical infrastructure is dependent on two particular interconnected physical and cyber-based control systems: supervisory control and data acquisition (SCADA) and distributed control systems (DCS).[18] The near-ubiquitous employment of these systems results from the clear benefits they bring to operational efficiency: they allow the remote operation and maintenance of critical infrastructures in real time.[19] These systems, however, are inherently vulnerable as their communication is carried out through a variety of media, including Ethernet, wireless, shared leased lines, and the Internet.[20] In addition, SCADA and DCS are also now built using commercial of-

---

[9] Paul W Phister Jr, 'Cyberspace: The Ultimate Complex Adaptive System', *The International C2 Journal* 4, no. 2 (2011 2010): 13.
[10] Perrow, *Normal Accidents: Living with High-Risk Technologies*, 3; Stevens, *Cyber Security and the Politics of Time*, 115.
[11] Perrow, *Normal Accidents: Living with High-Risk Technologies*, 3–4.
[12] Phister Jr, 'Cyberspace: The Ultimate Complex Adaptive System'.
[13] Saurabh Mittal, 'Special Issue: Cyber Complex Adaptive Systems: Methodologies, Paradigms, Tools and Technologies', *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 12, no. 2 (April 2015): 209, https://doi.org/10.1177/1548512915580762.
[14] Phister Jr, 'Cyberspace: The Ultimate Complex Adaptive System', 13.
[15] Clemente, *Cyber Security and Global Interdependence What Is Critical?*, 7.
[16] Clemente, v.
[17] Richard G. Little, 'Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures', *Journal of Urban Technology* 9, no. 1 (April 2002): 112, https://doi.org/10.1080/106307302317379855.
[18] United States Army, 'Cyberspace Operations Concept Capability Plan 2016-2028', 12.
[19] ENISA, 'Communication Network Dependencies for ICS/SCADA Systems', Report/Study, December 2016, 7, https://www.enisa.europa.eu/publications/ics-scada-dependencies.
[20] Patricia A.S. Ralston, James H. Graham, and Jeffrey L. Hieb, 'Cyber Security Risk Assessment for SCADA and DCS Networks', *ISA Transactions* 46, no. 4 (1 October 2007): 585, https://doi.org/10.1016/j.isatra.2007.04.003.

the-shelf (COTS) components, some of which have known security vulnerabilities.[21] The European Union Agency for Network and Information Security (ENISA) has identified a number of plausible attack scenarios involving the exploitation of these vulnerabilities. One scenario envisages an attacker compromising the systems by taking control of one or multiple assets in the network and thereby manipulating them all – an intrusion that could potentially cause blackouts or service cuts if it involves the energy grid. Another scenario concerns malware infections during SCADA system maintenance and upgrade processes.[22] If the state of one critical infrastructure depends on information transmitted through another critical infrastructure, then an attack on one SCADA system can potentially produce a cascading failure.[23]

Complex adaptiveness is a particular problem for risk societies because they value predictability. As Chapter 2 explained, an awareness of the unintended consequences of technological progress lies at the root of risk society reasoning. The heightened probability of accidents and failures in cyberspace will thus be particularly alarming to risk societies.

3.2.2 Operational characteristic 2: ease of proliferation

A second operational characteristic that creates uncertainty is the ease of proliferation of offensive cyber capabilities among actors in the international system. The concept of proliferation means the acquisition of a pre-existing or similar capability by an actor other than its creator.[24] Generally speaking, there is a higher likelihood of proliferation and diffusion of cyber capabilities in comparison to kinetic weapons. Cyber capabilities, unlike kinetic weapons, do not necessarily destroy themselves upon use, meaning that their components may be repurposed.[25] And once a cyber capability has been developed, it can often be reverse engineered, making it far cheaper and easier to manufacture other capabilities.[26] With the right malware analysis expertise, an adversary is able to draw inspiration from or reuse the techniques, tools, and procedures (TTPs) used in different stages of a previous attack.[27]

To take an example, the EternalBlue exploit was likely first developed by the NSA and subsequently stolen and leaked online by a hacker group called the Shadow Brokers. EternalBlue

[21] Ralston, Graham, and Hieb, 585.
[22] ENISA, 'Communication Network Dependencies for ICS/SCADA Systems', 7.
[23] Panayiotis Kotzanikolaou, Marianthi Theoharidou, and Dimitris Gritzalis, 'Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects', in *Critical Information Infrastructure Security*, ed. Sandro Bologna et al., Lecture Notes in Computer Science (Berlin and Heidelberg: Springer, 2013), 105.
[24] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 166.
[25] Steven M. Bellovin, Susan Landau, and Herbert S. Lin, 'Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications', *Journal of Cybersecurity* 3, no. 1 (2017): 65.
[26] Kello, *The Virtual Weapon and International Order*, 168.
[27] Attack stages include: initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, data collection, command and control, exfiltration, and final impact. See: The MITRE Corporation, 'Matrix: Enterprise | MITRE ATT&CK™', MITRE ATT&CK™, 2018, https://attack.mitre.org/matrices/enterprise/.

exploits the CVE-2017-0144 vulnerability in the Server Message Block (SMB) protocol, which is used in Windows machines to request files and print services from server systems over a network.[28] EternalBlue is therefore most useful for using remote services to move laterally within a network, thus enabling the fast spread of malware between systems.[29] Indeed, EternalBlue has been repurposed multiple times by groups other than the developer for the execution of widespread and damaging cyber attacks – most infamously in the cases of the WannaCry ransomware attack and NotPetya.[30]

In cases where the simple redeployment of an exploit or other technique is not possible – usually when a capability has been precisely designed to affect only one specific target – design emulation still remains an option for an aspiring proliferant.[31] This works by copying not lines of code, but the operation's design features (for example, the method of entry). The case that most notably comes to mind is Stuxnet. While the worm that targeted the programmable logic controllers at the Natanz nuclear facility was highly customised, and thus released its payload only within specific systems in the target facility, the broad attack tactics and technology were generic enough to be used against other targets by way of emulation.[32] Specifically, Stuxnet could serve as inspiration for designers of cyber attacks to exploit *physical* vulnerabilities in plant and control systems.[33] Exploiting flaws in the products and architecture of industrial control systems can be particularly attractive to an attacker because these vulnerabilities – unlike software vulnerabilities – cannot be patched and are therefore likely to remain exploitable for years.[34] Indeed, leaked NSA documents reveal that the Agency fears Iran will draw inspiration and operational ideas from western cyber attacks that targeted its infrastructure, including Stuxnet, Flame, and Duqu, to develop its own similarly sophisticated operations.[35]

The ease of proliferation has the effect of lowering the barriers to entry into the cyber domain for malicious actors. The multiplicity of offensive actors, from state agencies to hacker groups, has been studied extensively by scholars.[36] Previously weak actors, including non-state actors, no longer need to

---

[28] SentinelOne, 'Eternalblue | How the NSA-Developed Exploit That Just Won't Die', *SentinelOne* (blog), 27 May 2019, https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/.
[29] The MITRE Corporation, 'Technique: Exploitation of Remote Services - Enterprise | MITRE ATT&CK™', MITRE ATT&CK™, 2018, https://attack.mitre.org/techniques/T1210/.
[30] Raj Samani, Christiaan Beek, and Charles McFarland, 'An Analysis of the WannaCry Ransomware Outbreak', *McAfee Blog* (blog), 12 May 2017, https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/; Lily Hay Newman, 'The Leaked NSA Spy Tool That Hacked The World', *Wired Magazine*, 3 July 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.
[31] Kello, *The Virtual Weapon and International Order*, 168.
[32] Ralph Langner, 'To Kill A Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve', *The Langner Group*, November 2013, 4.
[33] Langner, 19.
[34] Langner, 19.
[35] Kim Zetter, 'The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks', *Wired*, 2 October 2015, https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/.
[36] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37, https://doi.org/10.1080/01402390.2014.977382; Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011); Jon R. Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack', *Journal of Cybersecurity* 1, no. 1 (27 November 2015): 53–67,

develop cyber capabilities from scratch; they are able to quickly take advantage of the time it takes to patch systems and redeploy previously used capabilities or simply purchase them on illegal marketplaces. The gains of intelligence agencies and cyber units that stockpile exploits can quickly be translated into losses if capabilities are stolen or "escape" in testing stages.

A related issue is the problem of arms control in cyberspace. Cyber capabilities do not lend themselves to quantitative estimation because of their non-physical nature and their frequent re-engineering to ensure their effectiveness against a constantly shifting attack surface.[37] Weak arms verification thus begets weak arms control, which in turn begets capability proliferation, leading to a vicious circle. The range of scenarios and threats that might arise from rampant proliferation is difficult to predict, posing a particular issue for risk societies which are especially sensitive to the risks of diverse conceivable risk scenarios.

3.3 Cyberspace and uncertainty: how operational characteristics can complicate responses

Having reviewed the operational characteristics of cyberspace that are especially problematic for risk societies because they create uncertainty and risk, let us now explore how they pose an obstacle to the application of meaningful responses to cyber attacks. First, this section will show that the complexity of the environment and the proliferation of capabilities raise the risk of misattribution and plausible deniability. Wanting to avoid these risks, risk societies will engage in lengthy and detailed attribution processes, which means that they will tend to run out of time to respond meaningfully. Second, it will explore how the complexity of the cyber domain increases the risks of unintended effects, including collateral damage, blowback, and escalation. Given that unintended effects are one of the risk society's greatest fears, an awareness of these increased risks will particularly constrain their response options.

3.3.1 Consequence 1: the attribution problem: the risk of misattribution and plausible deniability

The structural complexity of the cyber domain and the wide universe of possible perpetrators as a result of proliferation, coupled with availability of anonymity-enhancing tools and techniques such as the Tor network,[38] lengthen the forensic process of attributing attacks.[39] While scholars have shown

https://doi.org/10.1093/cybsec/tyv003; Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38, no. 2 (2013): 7–40, https://doi.org/10.1162/ISEC_a_00138.

[37] Erica D. Borghard and Shawn W. Lonergan, 'Why Are There No Cyber Arms Control Agreements?', *Council on Foreign Relations Net Politics* (blog), 16 January 2018, https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.

[38] Joss Wright, 'Regional Variation in Chinese Internet Filtering', *Information, Communication & Society* 17, no. 1 (2 January 2014): 131, https://doi.org/10.1080/1369118X.2013.853818.

[39] Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *The Cyber Issue*, Winter 2016, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

that, contrary to what was believed previously, technical attribution of a cyber incident is usually possible, the analysis of an operation within a narrow timeframe is nevertheless challenging even for well-resourced teams.[40] The complexity of cyber attribution therefore gives rise to the possibility that an operation may be incorrectly attributed or the possibility that the attacker will plausibly deny his involvement.

Societies high on the risk spectrum will care particularly about these possibilities. As we discussed, risk societies abhor uncertainty; they will generally not issue a meaningful response while there is even the slightest risk of misattribution or risk that an operation might be plausibly deniable, as this could lead to unintended and unpredictable consequences, including triggering an unwanted conflict or diplomatic standoff.[41] In addition, risk societies are more likely to want to engage in *public* attribution with the aim of establishing international rules of behaviour in cyberspace to "stabilize a particular interaction order," that is, to increase predictability.[42] They are also more likely to engage in *collective* public attribution, because this involves intelligence sharing between a number of states, which in turn increases certainty in the conclusion of the attribution process and decreases the risk of plausible deniability.[43]

Public attribution falls under the rubric of what Florian Egloff termed the "meaning-making process" of attribution, defined as the national security process concerned with the communication of the attribution judgement to others in order to exert political effects.[44] This process, however, can take even longer than technical attribution. Concerns about not revealing sensitive sources and methods that informed an intelligence assessment, the reliance on which is often a necessity due to the aforementioned tools and features that that help obfuscate an attack perpetrator's identity, are an important complicating factor in this regard.[45] Thus, the length of time that it takes risk societies to confidently and publicly attribute an operation to a single state actor often means that they aren't able to conclude the attribution process in the time they have to respond meaningfully (recall that swiftness is a key element of a meaningful response).

Some scholars have argued that the most damaging attacks can be more easily attributed because few actors are in possession of the type of capabilities needed to execute and benefit from

---

[40] Rid and Buchanan, 'Attributing Cyber Attacks'.
[41] Showcasing the desire to limit unpredictability in the cyber domain, NATO has stated that, "We all stand to benefit from a rules-based, *predictable*, open, free, and secure cyberspace [emphasis added]." Chapter 6 will discuss NATO's identity as a "risk community." See: NATO, 'Statement by the North Atlantic Council Concerning Malicious Cyber Activities', NATO, 3 June 2020, http://www.nato.int/cps/en/natohq/official_texts_176136.htm.
[42] Florian J. Egloff, 'Public Attribution of Cyber Intrusions', *Journal of Cybersecurity* 6, no. 1 (1 January 2020): 5, https://doi.org/10.1093/cybsec/tyaa012.
[43] For further elaboration of this point see, for example, a recent speech by the UK Attorney General: Jeremy Wright, 'Speech: Cyber and International Law in the 21st Century', GOV.UK, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[44] Egloff, 'Public Attribution of Cyber Intrusions'.
[45] Egloff, 3; Rid and Buchanan, 'Attributing Cyber Attacks'.

them.[46] Going against these analyses, the cases of WannaCry and NotPetya demonstrated that an attack's level of sophistication isn't necessarily the most reliable indicator of the perpetrator as neither the ransomware nor the delivery methods in these attacks were particularly sophisticated. In fact, cybersecurity researchers, having found numerous bugs in the WannaCry code, initially speculated that the malware had "escaped" from its authors in the development stages.[47] The element of WannaCry that was more advanced was the EternalBlue exploit, but, as we discussed, this NSA-developed exploit was simply repurposed after having been leaked online.[48] In both the WannaCry and NotPetya cases, the length of time that it took victim states to issue public attribution statements is evidence in itself of the complexity of the process, both from a technical and a political standpoint. The attacks took place in May 2017 and June 2017, respectively, but formal attribution statements were issued months later in December 2017 and February 2018, also respectively.[49]

3.3.2 Consequence 2: the risk of unintended effects: collateral damage, blowback, and escalation

Other considerations arising from operational uncertainty that can complicate the response calculus are first, the unintended effects of the initial attack, which can interfere with the victim's interpretation of the attack's intent and make it difficult to determine a timely response, and second and more important, an awareness of potential unintended effects of a (cyber) response, in terms of collateral damage, blowback, or escalation. The reflexive nature of risk societies and their strong awareness of the negative side effects of technological progress mean that the possibility of unintended effects will have a particularly strong paralysing effect on the response decision-making.

In kinetic military operations, collateral damage refers to physical damage to a civilian target or civilian deaths resulting from an offensive action.[50] The concept is key to the discussion of the principles of proportionality and distinction in the Geneva Conventions and there exists a well-defined methodology for assessing and anticipating collateral damage from conventional military actions.[51] The same is not true for the cyber domain, which complicates the response calculus of states that experience

---

[46] Lindsay, 'Tipping the Scales', 56.
[47] Elias Groll, 'Security Firms Tie WannaCry Ransomware to North Korea', *Foreign Policy* (blog), accessed 31 March 2020, https://foreignpolicy.com/2017/05/23/security-firms-tie-wannacry-ransomware-to-north-korea/.
[48] Amanda McKeon, 'WannaCry About NotPetya?', *Recorded Future* (blog), 10 July 2017, https://www.recordedfuture.com/podcast-episode-14/.
[49] Foreign and Commonwealth Office, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks', gov.uk, 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; White House, 'Statement from the Press Secretary', 15 February 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
[50] Sasha Romanosky and Zachary Goldman, 'Cyber Collateral Damage', *Procedia Computer Science* 95 (2016): 10–11.
[51] Wolff Heintschel von Heinegg, 'Proportionality and Collateral Damage', in *Max Planck Encyclopedia of Public International Law [MPEPIL]*, October 2015, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e2166; Romanosky and Goldman, 'Cyber Collateral Damage', 11.

cyber attacks, because there is greater potential for collateral effects in cyberspace than in physical space.[52] In fact, the high degree of interconnectedness between systems and between the external functions they support (operational characteristic 1) means that a cyber attack can cause indirect effects that surpass the direct effects on the target systems themselves. Cascading collateral damage can therefore impact vital activities across a wide range of interests and interfere with the interpretation of the attack.[53] The unplanned spread of malware and its highly unpredictable collateral damage will be a prominent concern among risk-conscious policymakers considering a cyber response.

A second problem arising from the high probability of unintended effects of operations in the cyber domain is that cyber retaliation can be counterproductive if the spread of malware or collateral damage is so substantial that it generates blowback. Blowback from a cyber response can happen in two ways. First, malware used in a retaliatory attack can inadvertently spread between machines and damage the retaliator's own infrastructure or that of allies. This can occur in the case of poorly customised capabilities, such as those targeting near-ubiquitous Windows operating systems.[54] An illustrative example of a cyber attack (not retaliatory in this case) having blowback effects is the NotPetya attack, which, like WannaCry, took advantage of the Windows EternalBlue exploit discussed earlier. While the attack was traced back to the Russian state, it was found to have affected large Russian companies, such as Rosneft, as well.[55] A second form of blowback occurs when a cyber attack targeting a single institution ends up disrupting assets in a public commons, such as nodes in the global financial system, due to the interconnectedness of computer systems.[56] Such a situation has not yet fully materialised, but hints at its occurrence exist. NotPetya, for instance, had a significant impact on global shipping and trade. Although the attack was meant to target systems in Ukraine, it brought Maersk, a company that carries one fifth of the world's entire shipping cargo, to a standstill for a period of two weeks.[57] NotPetya therefore represents a combination of two types of blowback.

Conscious of the potential for blowback, victims might be more cautious in responding to a cyber attack using the same means for fear of their retaliatory operation affecting their own (or allies') digital infrastructures. This is especially the case in countries that are more vulnerable to malware than their adversaries, having prioritised innovation and connectivity at the expense of systems security.[58]

The risks of blowback can produce self-restraint among risk societies even in the application of non-cyber responses, for example economic sanctions. Sanctions are a frequent choice of risk

---

[52] Romanosky and Goldman, 'Cyber Collateral Damage', 16.
[53] Kello, *The Virtual Weapon and International Order*, 198.
[54] Kello, 201.
[55] Andy Greenberg, 'The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired Magazine*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[56] Kello, *The Virtual Weapon and International Order*, 201.
[57] Greenberg, 'The Untold Story of NotPetya, The Most Devastating Cyberattack in History'.
[58] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st ed. (New York: Ecco, 2010), 189.

societies for responding to cyber attacks as they are perceived to be more controlled, less destructive, and therefore less escalatory than offensive cyber operations.[59] At the same time, they can produce blowback effects because of the interconnectedness of the global economy.[60] In the particular case of the United States, the frequent resort to the application of sanctions for coercive purposes has led states to seek to reduce their dependence on the US dollar and develop alternatives to the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[61] Such actions could eventually even have the effect of displacing the United States from its dominant position in the international financial system.[62]

Returning to the possible unintended effects of a cyber response, a third such effect is escalation. Inadvertent or accidental escalation can occur when one party's actions are interpreted as escalatory by the other party to a conflict and this party issues a stronger counter-response.[63] As Ben Buchanan wrote, the dilemmas of interpretation of intent are particularly pronounced in cyberspace.[64] Accidental escalation can happen as a result of signalling issues, which are born from the fact that cyberspace is constantly full of activity (as described under operational characteristic 2 – proliferation and diversity of actors), making it difficult for a state to recognise clear signals of what an adversary wants to achieve through a cyber attack.[65] Additionally, as we discussed, problems of interpretation of attacks may result from excessive damage to unintended targets; it is not easy to quickly design cyber operations that are fully predictable and carefully calibrated in terms of their impact.[66] Even in cases where a risk society executes a precisely targeted operation, as a result of its strong sense of vulnerability in cyberspace (an outgrowth of the awareness of negative side effects of technological progress), it will worry about the adversary's counter retaliation and tend to imagine worst-case scenarios.

Altogether, the characteristics of the cyber domain – including the system's technical complexity and the ease of proliferation and the consequences of these in terms of breeding uncertainty in attribution and uncertainty of the effects of a cyber response – are likely to lead risk-conscious

---

[59] David C. Gompert and Hans Binnendijk, 'The Power to Coerce: Countering Adversaries Without Going to War' (Santa Monica, CA: RAND Corporation, 3 March 2016), 31, 32, https://www.rand.org/pubs/research_reports/RR1000.html.
[60] Gompert and Binnendijk, 32.
[61] Erica Borghard, 'Economic Sanctions Should Not Always Be the Go-to Foreign Policy Tool' (Washington, D.C.: Atlantic Council, 22 February 2021), https://www.atlanticcouncil.org/content-series/reality-check/reality-check-2-economic-sanctions-should-not-always-be-the-go-to-foreign-policy-tool/; Gabriel Crossley and Katya Golubkova, 'Explainer-China, Russia Vulnerable to Dollar Risks as Sanctions from West Multiply', *Reuters*, 23 March 2021, https://www.reuters.com/article/uk-china-russia-dollar-explainer-idUKKBN2BF1JB.
[62] Borghard, 'Economic Sanctions Should Not Always Be the Go-to Foreign Policy Tool'.
[63] Herbert Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', *Strategic Studies Quarterly* 6, no. 3 (2012): 52–53.
[64] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (London: Hurst & Company, 2016), 76.
[65] Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', 57.
[66] Lin, 53; Bellovin, Landau, and Lin, 'Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications', 266; Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 310.

policymakers towards restraint in the design of individual responses, or even the decision not to respond at all. In their general approach to cyberspace, they will also differ from threat societies whose focus is consumed by one particular actor. Given the uncertainties of the domain and the perceived risks of a response, risk societies are likely to place much more emphasis in their cyber strategies on risk management practices that minimise as much as possible the occurrence of cyber attacks and, if that fails, seek to manage their harmful consequences.

3.4 Risk management practices

Drawing from the risk management literature, we can identify three main practices that risk societies are likely to carry out in an attempt to manage risk and uncertainty in the cyber domain: preventive action, increasing resilience, and consequence management. These practices will form a central pillar through which risk societies address cyber challenges but should not be understood as a response to individual cyber attacks that substitute for punishment. They are not intended to influence the resolve of the attacker to engage in attacks, but rather are employed by risk societies to mitigate as much as possible the scale and effects of hostile operations on digital infrastructures, while maintaining an awareness that complete security is unattainable. The analysis now turns to a discussion of these practices.

3.4.1 Preventive action

Prevention in the cyber domain is the go-to practice for risk societies seeking to mitigate the risk of future attacks. Preventive action and the related, albeit definitionally separate, concept of pre-emption, are often associated with the Bush Doctrine, reigniting debates about the United States' invasion of Iraq in 2003. The concept of preventive action, however, goes back at least far as Thucydides' account of the Peloponnesian War in the fifth century B.C. when the Spartans reasoned that Athens had to be eliminated as a potential threat before it grew too powerful.[67] To make the concept of prevention more useful in a cyber context, we must first distinguish between prevention and pre-emption, and secondly between a preventive war, a preventive strike, and preventive action.

The distinction between preventive and pre-emptive strategies centres on timing: a pre-emptive strike takes place when an attack is credibly imminent.[68] The defender is faced with a scenario of either striking first or being on the receiving end of an attack.[69] Scholars have argued that the so-called Bush

[67] Thomas M. Nichols, *Eve of Destruction: The Coming Age of Preventive War* (Philadelphia: University of Pennsylvania Press, 2008), 5.
[68] Nichols, 5; Colin S. Gray, *National Security Dilemmas: Challenges and Opportunities*, 1st ed., Book Collections on Project MUSE (Washington, D.C.: Potomac Books, 2009), 223, https://muse.jhu.edu/book/41059/.
[69] Gray, *National Security Dilemmas: Challenges and Opportunities*, 218.

Doctrine was in fact a strategy of prevention, rather than pre-emption, as its proponents emphatically claimed.[70]

Estimating the immediacy of an attack is difficult and often subjective even in the physical domain, which has historically limited the usefulness of "imminence" as a guide to action.[71] In the cyber domain, where signalling is impaired and there are often no visible signs of attack preparation like troops amassing at borders, this is even more difficult. On top of the lack of warning, the attacks themselves take place within milliseconds. Pre-emption is therefore often not a viable strategy in the cyber domain. Prevention, however, can be viable.

Prevention is a strategy designed to eliminate potential threats or thwart the adversary's acquisition of threatening capabilities.[72] Often, a preventor will act in order to stop an enemy from shifting the balance of power or engage in actions that would be intolerable to the preventor.[73] Importantly, prevention implies an unwillingness to tolerate risk and an intention to control the external security environment.[74] Prevention therefore often involves a great deal of prediction of future threats amid uncertainty. It leaves far more choice for the defender than pre-emption, where it is the adversary that controls the timing having already decided to launch an attack.[75]

The force that often needs to be used as part of a strategy of prevention in the physical domain carries significant risks of its own, which may often outweigh its benefits.[76] This balance is not the same in the cyber domain because preventive action in this environment is, at least so far, non-violent. This is where we arrive at the distinction between preventive strikes, preventive war, and preventive action. A preventive strike is a short duration military action to remove an adversary's capability; this can be done through covert operations, interdictions, or targeted killings.[77] A preventive war is an extended military engagement designed to defeat the enemy before the enemy has had the time to grow into a formidable threat to the preventor. In the case of preventive war, policymakers decide it is better to fight "today" than "tomorrow," when the enemy might be in a better position to alter the balance of power.[78]

In the conventional military domain, both a preventive strike and a preventive war involve some degree of violence. In the cyber domain, however, eliminating a potential threat can often be achieved

---

[70] Michael W. Doyle, 'Striking First', in *Striking First: Preemption and Prevention in International Conflict*, ed. Stephen Macedo, University Center for Human Values Series (Princeton, NJ: Princeton University Press, 2008), 25, https://ezproxy-prd.bodleian.ox.ac.uk/login?url=https://www.jstor.org/stable/10.2307/j.ctt7t7md; Nichols, *Eve of Destruction: The Coming Age of Preventive War*, 9; Richard K. Betts, 'Striking First: A History of Thankfully Lost Opportunities', *Ethics & International Affairs* 17, no. 1 (March 2003): 17–24, https://doi.org/10.1111/j.1747-7093.2003.tb00414.x; Gray, *National Security Dilemmas: Challenges and Opportunities*, 222.
[71] Nichols, *Eve of Destruction: The Coming Age of Preventive War*, 8.
[72] Nichols, 8; Doyle, 'Striking First', 5.
[73] Gray, *National Security Dilemmas: Challenges and Opportunities*, 218.
[74] Gray, 226.
[75] Gray, 218.
[76] Gray, 228.
[77] Nichols, *Eve of Destruction: The Coming Age of Preventive War*, 7–13.
[78] Gray, *National Security Dilemmas: Challenges and Opportunities*, 227.

by non-violent actions such as taking an adversary's attack infrastructure offline, exploiting adversary vulnerabilities in a way that consumes their attention and resources, or releasing information about exploits used by an adversary into the public domain. It may also involve operating in adversaries' networks, or so-called "red space," and can result in some level of destruction, but mostly of data. It therefore does not carry the same probability of violence or loss of life as in the physical domain. Thus, preventive *action* is a more accurate term for such activity in cyberspace.

3.4.2 Increasing resilience

Increasing resilience is defined as developing the capacity to "withstand, recover from, and adapt to external shocks."[79] For our purposes here, the most important feature of resilience-building is that it takes place *before* an incident has happened and includes technical measures that can reduce harm in an automated and pre-programmed manner. *After* an incident has taken place, states will seek to manage the attack's harmful consequences, which is a human-oriented effort because it involves analysis and decision-making during the event itself (as we will discuss next).

Examples of resilience-building in the cyber domain include the introduction of intrusion detection technologies, improving general cyber "hygiene" through, for example, introducing two-factor authentication, conducting regular network penetration tests, installing "patches," updating operating systems, maintaining robust backup procedures and, more generally, building systems that can withstand attacks.[80] Some might argue that resilience-building (and also preventive action) are no different to the implementation of mechanisms for deterrence by denial.[81] Indeed, if the defences are known to the adversary, the techniques used in risk management may also serve deterrence purposes, that is, they may have the psychological effect of dissuading the adversary from launching an attack in the first place.[82] Yet, it is important to recognise that in building resilience, risk societies will not hold

---

[79] Benoît Dupont, 'The Cyber-Resilience of Financial Institutions: Significance and Applicability', *Journal of Cybersecurity* 5, no. 1 (1 January 2019): 2, https://doi.org/10.1093/cybsec/tyz013.

[80] Lindsay, 'Tipping the Scales', 54; Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (1 January 2017): 57, https://doi.org/10.1162/ISEC_a_00266.

[81] Scholarly definitions of deterrence by denial broadly cluster around the notion of the "threat that effective defences will defeat an attack" or a promise to prevent the opponent from achieving their objectives Lindsay, 'Tipping the Scales', 53; James J. Wirtz, 'How Does Nuclear Deterrence Differ from Conventional Deterrence?', *Strategic Studies Quarterly* 12, no. 4 (2018): 70..

[82] Some scholars might dispute this. Michael Fischerkeller, for example, argued that US policymakers have often viewed increasing resilience incorrectly as part of a strategy of deterrence by denial. According to Fischerkeller, deterrence by denial threatens the aggressor with a war of attrition, making aggression unprofitable – it has little to do with hardening the defence surface and more to do with capabilities. He concluded that increasing resilience can instead be better understood as being part of a *defence* strategy, that is, diminishing an adversary's ability to inflict damage, rather than a *denial* strategy, which, according to Fischerkeller, is structurally impossible in cyberspace. See: Michael P. Fischerkeller, 'The Structural and Strategic Imperative: The Need for Persistent Engagement' (Washington, D.C.: IDA Institute for Defense Analyses, October 2018), https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

deterrence as their primary aim. Their objective instead will be to prevent at least some proportion of the attacks from penetrating their systems.

Spurred by their sense of perpetual insecurity in the face of technological developments, risk societies will also be particularly attuned to the fact that in the current state of play, where most critical systems depend on computer networks, the sheer number of important targets that require advanced defences and constant system updates may simply overwhelm defenders. And they will refer to the recent empirical record of cyber attacks to reinforce these beliefs. The case of EternalBlue illustrates how difficult it is to implement effective defences of digital terrain: despite Microsoft issuing patches for the vulnerabilities in the SMBv1 protocol in March 2017, the use of EternalBlue grew continuously and reached historic peaks in use as late as May 2019.[83] Acutely aware of these challenges brought by modernisation, risk societies will therefore also prioritise planning how they will handle the consequences of damaging cyber intrusions.

3.4.3 Consequence management

In cases where a cyber operation does succeed in breaching a system, states will engage in consequence management. Actions under consequence management are those taken during the course of or in the aftermath of an incident to reduce the impact of its effects and aid recovery.[84] While bolstering resilience intends to increase the security of systems to prevent cyber attacks from breaching them and, if that fails, trigger previously implemented measures that will allow for their quick restoration, consequence management is human oriented: it involves decision-makers analysing and addressing an already ongoing cyber attack in such a way as to prevent further loss or, in the aftermath of an attack, alleviate damage. An example of consequence management is cooperation among government officials in different countries to disrupt foreign-based botnets during the course of an attack.

The following table summarises how the features of the cyber domain interact with the concerns of risk societies.

[83] Ondrej Kubovič, 'EternalBlue Reaching New Heights since WannaCryptor Outbreak', WeLiveSecurity, 17 May 2019, https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/.
[84] European Commission, 'Annual Work Programme 2010: Prevention, Preparednesss and Consequence Management of Terrorism and Other Security Related Risks', European Commission, 2010, 2, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/financing/fundings/pdf/cips/work_programme_2010_en.pdf.

Table 5: The interaction between the operational characteristics of cyberspace and risk society sensitivities

Risk society characteristics	How the operational environment amplifies risk sensitivities
• *Reflexive:* concerned with unintended consequences arising from technological progress.	• Technological progress has created a dependency on cyberspace. Previously regarded a major generator of economic wealth and prosperity, technological progress is now regarded as a source of vulnerability.
• *Particularly preoccupied with uncertainty and risks:* diverse, potential, uncertain scenarios (often worst-case ones), usually connected to technological progress, that are an unintended result of one's own actions or decisions.	• Higher risk of unintended consequences from one's own actions, such as collateral damage, conflict escalation, and blowback, due to the environment's complex adaptiveness and ease of proliferation. • Higher risk of misattribution and plausible deniability. • Scenarios are particularly difficult to predict as a result of complex adaptiveness and ease of proliferation.
• *Proactive in the application of preventive measures and/or paralysed decision-making in reaction to an incident:* likely to engage in preventive measures to manage risks and to experience paralysis in the aftermath of an incident (as opposed to taking a strong reactive approach).	• The difficulty of conceiving future attack scenarios incentivises prevention. • Prevention in the cyber domain is non-violent normally covert. Thus, it is less risky than in the kinetic domain.

3.5 Threat societies

Concerns about operational uncertainty will not feature significantly in the decision-making processes on how to respond in threat societies. This is because such states, in addition to being culturally predisposed towards risk-acceptance, usually have a firm focus on a single, well-defined adversary that they perceive to be an existential threat. Security situations are therefore analysed primarily through the prism of the relationship with that primary adversary and the adversary's perceived identity, rather than with reference to the diverse worst-case scenarios that could arise as an unintended consequence of that state's actions. This means that threat societies tend to be risk-acceptant; their view is that, due to the existence of a threatening adversary, their country is in a

permanent state of danger anyway – thus risks are unavoidable. The preoccupation with one well-defined existential threat effectively crowds out attention to diverse risks or relegates them to a lower importance.

In reacting to a cyber attack, especially if the attack's perpetrator is the main geopolitical adversary, such states are more likely to prioritise signalling resolve to punish, while not devoting much attention to the operational features of cyberspace, such as the potential for cascading harm or particular vulnerability to blowback. Indeed, cyberspace is likely to be seen as "just another battlespace" in which the state's conflict with its primary adversary unfolds, rather than as a strategically distinct domain. Thus, the logic employed in dealing with hostile cyber attacks is likely to be similar to the strategic thinking used in other domains. As such, these states, not paying significant attention to the unique properties of cyberspace, will remain *reactive* in their security posture. This does not mean that threat societies will not use preventive practices, resilience-building, and consequence management as well; what it means, rather, is that these practices will not arise from intense attention to the operational particularities of cyberspace (as they do in risk societies) and are therefore not likely to form the centrepiece of threat societies' approach to conflict in cyberspace. Moreover, because these states are not likely to have developed strategies that are particular to the cyber domain, they will integrate these practices into more general national security strategies such as deterrence.

Threat societies embedded in risk communities, as Chapter 1 discussed, will be expected to defer to the risk sensitivities of the risk community (which will correspond to those of risk societies detailed earlier).

3.6 Conclusion

This chapter reviewed the sources of uncertainty in the cyber domain – the complex adaptiveness of cyberspace as a system and the ease of proliferation of capabilities – and explained why they pose a particular obstacle to risk societies. It showed that there are two particular risks that stem from these operational characteristics – the risk of misattribution and plausible deniability and the risk of unintended effects, particularly escalation, which in risk-sensitive states impede the application of meaningful punishment for cyber attacks. The chapter noted that, as a result of these obstacles, societies high on the risk spectrum are likely to emphasise risk management practices, including preventive action, resilience-building, and consequence management, as the main strategic tools to address the uncertainties of the cyber domain. Threat societies will be different. Their risk acceptant culture and firm focus on a single perceived existential threat will mean that they are unlikely to recognise cyberspace as a strategically distinct domain and will employ similar strategic thinking as in other domains. This means that the inherent uncertainty of cyberspace will not feature heavily in their decision-making on responses.

This chapter's illustration and elaboration of the conceptual framework developed in Chapter 2 will help to elucidate the empirical case studies of ensuing chapters. The case studies will seek to demonstrate that the risk framework can be applied to explain varying patterns of state response to cyber attacks. The analysis in the case studies will also seek to identify whether the state in question employed risk management practices in the cyber domain.

Chapter 4
The United States: A Risk Manager in a Networked World

[W]e're a cheap date when it comes to cyber. … People can go after us … and not really expect much in the way of a response, whether it's the Chinese OPM hack or the Russian attack on our elections or … Anthem, Blue Cross, Sony Pictures.

US Senator Angus King, 2019[1]

For over 20 years, nation-states and non-state actors have used cyberspace to subvert American power, American security, and the American way of life. Despite numerous criminal indictments, economic sanctions, and the development of robust cyber and non-cyber military capabilities, the attacks against the United States have continued. The perpetrators saw that their onslaught damaged the United States without triggering a significant retaliation.

Cyberspace Solarium Commission, 2020[2]

4.1 Introduction[3]

As Chapter 1 outlined, despite formally adopting a strategy of deterrence[4] and promising to respond to hostile cyber activity because of its significance to national security interests,[5] neither the Obama administrations nor the Trump administration actually issued meaningful punishments. In 2014, still as a nominee for the Commander of US Cyber Command, Vice Admiral Michael Rogers told the Senate

[1] Sydney J. Freedberg Jr., 'A "Solarium" For Hacking: Sen. King Launches Cyber Strategy Panel', Breaking Defense, 13 May 2019, https://breakingdefense.com/2019/05/a-solarium-for-hacking-sen-king-launches-cyber-strategy-panel/.

[2] Angus King and Mike Gallagher, eds., 'United States of America Cyberspace Solarium Commission', March 2020, 1, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[3] Parts of this chapter were published in: Monica Kaminska, 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks', *Journal of Cybersecurity* 7, no. 1 (9 March 2021), https://doi.org/10.1093/cybsec/tyab008.

[4] For official US documents stating the adoption of the strategy of deterrence in cyberspace see: The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', May 2011, https://doi.org/10.1037/e688502011-001; U.S. Department of Defense, 'Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934', November 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf; U.S. Department of Defense, 'The Department of Defense Cyber Strategy', April 2015, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf; The White House, 'Report on Cyber Deterrence Policy', 2015, https://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf; The White House, 'National Cyber Strategy of the United States of America', September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; U.S. Department of Defense, 'Summary: Department of Defense Cyber Strategy', 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[5] Michael Daniel, 'Our Latest Tool to Combat Cyber Attacks: What You Need to Know', The White House, 1 April 2015, https://obamawhitehouse.archives.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know.

Armed Services Committee: "I believe the U.S. may be considered an easier mark because our own processes and criteria lead the adversary to believe, rightly or wrongly, that we do not have the will to respond in a timely and proportionate manner."[6] Despite holding as his number one aim the establishment of costs for attacking the United States in cyberspace, in 2018, shortly before leaving his position, Rogers admitted that he had not been granted additional authorities under the Trump administration to respond to cyber attacks and disclosed that, "[w]e're taking steps, but we're probably not doing enough."[7] One of the purposes of this chapter is therefore to set up a comparative exercise in the context of the whole thesis: showing here that cyber attacks that significantly affected national security interests did not elicit a meaningful response will allow for this case to later be contrasted with the Israeli case in which similarly significant cyber attacks did elicit such a response.

Another purpose of this chapter is to determine whether the risk framework helps explain the posture of the United States towards foreign cyber attacks. According to the framework, we can expect that risk societies, which are particularly sensitive to uncertainty, will fail to punish cyber attacks meaningfully because they will be unwilling to accept the risks that stem from the operational environment of the cyber domain. The framework holds that they will be particularly concerned with two operational characteristics, cyberspace as a "complex adaptive" system and the ease of proliferation of cyber capabilities, and the risks these create in terms of the risk of misattribution or plausible deniability and the risk of unintended effects, including inadvertent escalation, collateral damage, and blowback.

This chapter, focusing on events occurring between 2008 (the beginning of the first Obama administration) and September 2020,[8] will argue that the reason the United States did not punish meaningfully is because, in accordance with the risk society tenets, it was sensitive to the risks of a potential meaningful response, which policymakers saw as arising from the features of the operational environment. The discussion will show that US policymakers exhibited concerns with both operational characteristics highlighted in the risk framework: complex adaptiveness and the proliferation of capabilities. It will also show that the attribution risks and the risk of unintended effects, including collateral damage, blowback, and inadvertent escalation, were seen as obstacles to the implementation of meaningful punishment (the latter particularly so in the case of a cyber punishment). Moreover,

---

[6] Senate Committee on Armed Services, 'Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command', 2014, https://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

[7] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Scribe UK, 2018), xix.; Rogers cited in: Aaron Blake, 'Analysis: NSA Director Mike Rogers's Remarkable Comments about Trump's Russia Efforts — or Lack Thereof', *The Washington Post*, 28 February 2018, https://www.washingtonpost.com/news/the-fix/wp/2018/02/27/nsa-director-mike-rogerss-careful-indictment-of-trumps-anti-russia-efforts/.

[8] This case study is time-limited to the two Obama administrations and the Trump administration up until September 2020, when the data collection was completed. It therefore does not analyse developments under the Biden administration. The reason for this scoping limit is methodological: examining the decisions made by the current Biden administration risks being ahistorical because the administration could reverse itself at any moment. The conclusion chapter of this thesis briefly discusses developments after September 2020.

aligning with the expectations of the analysis in Chapter 3, the United States also implemented cyber risk management practices, including increasing resilience, consequence management, and preventive action. Preventive action was especially prioritised during the Trump administration as a direct consequence of policymakers' characterisation of the operational space as an environment of "constant contact," which can be seen as an extension of the understanding of cyberspace as a complex system.

The analysis of this chapter will proceed as follows. Section 4.2 will provide a historical overview of significant cyber incidents affecting the United States and illustrate that although these cyber operations created significant effects for national security, the responses to them, under both President Barack Obama and President Donald Trump, were marked by weakness. Section 4.3, applying the risk society framework, will identify the societal, historical, and cultural factors that led to the emergence of risk sensitivity in the United States. Section 4.4 will use the risk framework presented in Chapter 2 and Chapter 3 to discuss the United States' responses to cyber attacks in the context of the risk society. It will first show that US policymakers were, in accordance with the expectations of the framework, concerned about the operational characteristics of the cyber domain in terms of its complex adaptiveness and the ease of proliferation of cyber capabilities. It will then discuss how the risk of misattribution posed an obstacle to meaningful punishment in the case of NotPetya. Next, it will analyse how policymakers' concern about the risk of unintended effects, including collateral damage, inadvertent escalation, and blowback, posed an obstacle to meaningful punishment in the case of the 2011-2013 Iranian distributed denial of service (DDoS) attacks (Operation Ababil), the 2014 Sony hack, and the 2016 Democratic National Committee (DNC) hack and election interference. Section 4.5 will delineate how the United States reacted to the challenges posed to it by cyberspace by implementing practices of risk management, which included increasing resilience, consequence management, and preventive risk management. Section 4.6 will conclude that the risk society indeed provides a "unifying framework"[9] for understanding US responses to cyber operations and its approach to cyber conflict more generally.

4.2 An overview of US cyber victimhood

The following discussion will provide a brief overview of the most significant cyber attacks that have affected the United States since 2008: Operation Ababil, the Sony Pictures hack, the DNC hack and election interference, and NotPetya. The purpose of this discussion is to illustrate that the attacks created significant effects for US national security, yet they were met with weak punitive responses.

[9] Christopher Coker, *War in an Age of Risk* (Cambridge: Polity Press, 2009), 66.

Operation Ababil was a long campaign of DDoS attacks inflicted against 46 institutions in the US financial sector, lasting 176 days from December 2011 until May 2013.[10] The significance of the attacks was underscored by the fact that American officials had long worried about an event that might further undermine the already (post-2008 financial crisis) shaken consumer confidence in the banking sector, which forms the backbone of the US economy and is a means of American power projection abroad.[11] The DDoS operation involved swamping and overwhelming the servers of multiple banks and financial institutions, including the New York Stock Exchange, Bank of America, and Chase Bank, with meaningless requests using a network of computers, called a botnet, thus preventing them from functioning. The strength of the attack was notable: at times it reached 140 gigabytes per second, which is three times the entire operating capacity of one targeted bank.[12] According to US House Intelligence Committee Chairman Mike Rogers, the attacks stressed US telecommunications and financial services infrastructure "to a dangerous level."[13] Hundreds of thousands of customers were unable to access their bank accounts online and the attacks cost the banks tens of millions of dollars in remediation costs.[14] General Keith Alexander, the director of the NSA at the time of the attacks, cautioned that if the United States didn't "do something," the "disruptive and destructive attacks on our country [would] get worse."[15]

There was no immediate reaction from the Obama administration. A leaked National Security Agency (NSA) correspondence with the UK Government Communication Headquarters (GCHQ) from 2013 stated that "senior officials in the Iranian government are aware of the [DDoS] attacks" and that the "NSA expects Iran will continue this series of attacks, which it views as successful, while striving for increased effectiveness by adapting its tactics and techniques to circumvent victim mitigation attempts."[16] In light of the clear expectation of further damaging attacks, the lack of response is all the more surprising.

The highly restrained reaction to the Iranian operation in fact came years later, in 2016, when the US Attorney General announced charges against seven Iranians working for two companies that had

[10] FBI, 'Iranians Charged with Hacking U.S. Financial Sector', Federal Bureau of Investigation, 24 March 2016, https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.
[11] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 153–54.
[12] Buchanan, 157.
[13] Joseph Menn, 'Cyber Attacks against Banks More Severe than Most Realize', *Reuters*, 18 May 2013, https://www.reuters.com/article/us-cyber-summit-banks-idUSBRE94G0ZP20130518.
[14] The United States Department of Justice, 'Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities', 24 March 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.
[15] Alexander cited in: Andrea Shalal-Esa, 'Top General Says U.S. under Constant Cyber Attack Threat', *Reuters*, 15 May 2013, https://www.reuters.com/article/us-cyber-summit-alexander-idUSBRE94D12L20130515.
[16] National Security Agency, 'Iran - Current Topics, Interaction with GCHQ', 12 April 2013, https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/.

executed the attacks on behalf of the Iranian Revolutionary Guard Corps.[17] By the US government's own admission, these "were no ordinary crimes, but calculated attacks … designed specifically to harm America and its people."[18] The extent to which the indictment will ever yield any real consequences is, however, doubtful. There is a low likelihood that the charged Iranian operators will ever face an American court, making the US Justice Department's actions largely symbolic.[19] Moreover, given the enormous delay in the response, it is almost certain that by 2016 "the idiom of reprisal," to use Schelling's language, had been lost.[20]

Barely a few months after Operation Ababil had finally ceased, the United States became the target of another large state-sponsored operation in 2014. This time it struck at another area of US economic interests: the entertainment industry. Reacting to the upcoming release of a satirical film about North Korea's leader Kim Jong-un, North Korean military hackers launched a months-long digital assault on Sony Pictures Entertainment, a California-based company, which disabled about three-fourths of its computer systems and cost Sony up to $35 million in damages.[21] Moreover, the hackers leaked unreleased films and confidential information and emails, which resulted in the dismissal of the company's co-chairwoman, Amy Pascal, and created lasting reputational damage to the American film-making industry.[22] Following the incident, the president publicly attributed the operation to North Korea and promised that the United States would "respond proportionately," "in a place and time and manner that we choose."[23] Obama's unyielding tone led to expectations that this would be the first time the United States would retaliate against a cyber attack.[24] In January 2015, the US Treasury announced economic sanctions against 10 senior North Korean officials and three government entities. However, having been imparted on one of the most heavily sanctioned regimes on earth, their impact was largely

[17] The United States Department of Justice, 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector', The United States Department of Justice, 24 March 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.
[18] The United States Department of Justice, 'Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities'.
[19] David E. Sanger, 'U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam', *The New York Times*, 24 March 2016, sec. World, https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html.
[20] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008), 141–45.
[21] Jack Goldsmith and Stuart Russell, 'Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations' (Stanford, CA: Hoover Working Group on National Security, Technology, and Law, 5 June 2018), 7, https://lawfareblog.com/strengths-become-vulnerabilities-how-digital-world-disadvantages-united-states-its-international-0; David E. Sanger and Nicole Perlroth, 'U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing', *The New York Times*, 26 April 2020, sec. World, https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.
[22] Buchanan, *The Hacker and the State*, 175–81.
[23] David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, 'Obama Vows a Response to Cyberattack on Sony', *The New York Times*, 19 December 2014, sec. World, https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html.
[24] Sanger, Schmidt, and Perlroth.

symbolic; all the entities had already been sanctioned previously.[25] Obama administration officials who designed the response themselves acknowledged that the sanctions had been "ridiculously weak."[26] And although the administration had previously promised that sanctions would be only the first step of a robust response, no further punitive actions entered into public knowledge.[27]

The response to the next major incident, the DNC hack during the 2016 presidential elections, is perhaps the most well-known example of the failure to deliver a meaningful punishment. Two months after the intrusions were detected, in September 2016, Obama delivered a warning to Russian President Vladimir Putin at the Group of 20 summit in China, cautioning that continued Russian operations to influence the election would be punished.[28] When the activities didn't stop, the president followed up with Putin on the Moscow-Washington hotline in October, reportedly to communicate US resolve.[29] There was also evidence that the administration had been working on a project that would insert "cyber weapons" into Russia's infrastructure, ready to be used in a retaliatory response.[30] All of this shows that Washington recognised that Russia's actions were continuing, despite the warnings. Yet, the administration ultimately reacted in the form of hastily applied diplomatic and economic sanctions and indictments in December. Daniel Friend, who oversaw the US government's sanctions policy under Obama, disclosed that officials knew the response was not strong enough to dissuade Russia from further attacks (which also indicates the existence of some additional consideration that prevented them from implementing stronger measures). "The Obama administration – in my view, and I was in it … – did not respond with adequate strength to the Russian interference in our elections … What we did in December 2016 was a very light set of sanctions, which I feel were frankly inadequate … those sanctions are not apt to be terribly effective, and we knew it." Friend concluded that, in his opinion, "the Russians understood it [the response] as inadequate."[31]

An extensive and long-awaited report on election interference in 2019 from Special Counsel Robert Mueller confirmed that "[t]he Russian government interfered in the 2016 presidential election

---

[25] David Francis, 'Obama Slams North Korea With Sanctions for Sony Hack', *Foreign Policy* (blog), 2 January 2015, https://foreignpolicy.com/2015/01/02/obama-slams-north-korea-with-sanctions-for-sony-hack/.
[26] Obama administration officials referenced in: Sanger, *The Perfect Weapon*, 150.
[27] Francis, 'Obama Slams North Korea With Sanctions for Sony Hack'.
[28] Julie Hirschfeld Davis and David E. Sanger, 'Obama Says U.S. Will Retaliate for Russia's Election Meddling', *The New York Times*, 15 December 2016, https://www.nytimes.com/2016/12/15/us/politics/russia-hack-election-trump-obama.html.
[29] William Banks, 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0 Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', *Texas Law Review* 95, no. 7 (2017): 1487–1514.
[30] Greg Miller, Ellen Nakashima, and Adam Entous, 'Obama's Secret Struggle to Punish Russia for Putin's Election Assault', *The Washington Post*, 23 June 2017, https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.858072115a9a.
[31] Daniel Friend cited in: Michael Isikoff, 'Ex-Sanctions Czar Bashes Obama Administration's "weak" Response to Russian Interference', Yahoo News, 20 April 2018, https://www.yahoo.com/news/ex-sanctions-czar-bashes-obama-administrations-weak-response-russian-interference-122944195.html.

in sweeping and systematic fashion."[32] What the Russians had intended to do was not just influence the vote, but undermine confidence in the election itself, with serious implications for American democracy.[33] The US Office of the Director of National Intelligence (ODNI) made it clear that election meddling was a means for "Russia to advance its interests both overtly and covertly." On this basis, the ODNI was concerned about the "increasingly damaging effects of cyber operations" and assessed that the greatest cyber threats to the United States (Russia, China, Iran, and North Korea), "will work to use cyber operations to achieve strategic objectives *unless they face clear repercussions for their cyber operations* [emphasis added]."[34]

Despite these revelations, the Trump administration's response was no more muscular than the Obama administration's. Rogers, by then Commander of Cyber Command and Director of the NSA, admitted that the Russians "haven't paid a price at least that's sufficient to get them to change their behaviour."[35] The rationale for a meaningful punitive response seemed clear: not punishing Russia would likely embolden Putin's government further and result in more damaging attacks. This sentiment was summarised by General H. R. McMaster, President Trump's National Security Advisor: the failure to impose costs meant that "the Kremlin's confidence [in targeting us again] is growing."[36]

One more operation merits mentioning here: NotPetya, an attack which likely targeted Ukraine, but spread globally like wildfire in 2017. When publicly attributing the operation to Russia, the US government described it as "the most destructive and costly cyber attack in history" and stated that "[t]his was also a reckless and indiscriminate cyber attack that will be met with international consequences."[37] Tom Bossert, the US Homeland Security Advisor at the time, commented on NotPetya: "[w]hile there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory." He emphasised: "[t]hat's a degree of recklessness we can't tolerate on the world stage."[38]

The fastest propagating piece of malware on record, NotPetya, as Bossert noted, was marked by its recklessness and destructiveness: an attack which had started with a breach of a Ukrainian accounting software firm, ended up spreading globally, paralysing a number of multinationals,

---

[32] Robert S. Mueller III, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election' (Washington, D.C.: U.S. Department of Justice, March 2019), 1, https://www.justice.gov/storage/report.pdf.
[33] Author interview with Chris Inglis, 30 September 2020.
[34] Office of the Director of National Intelligence, 'Worldwide Threat Assessment of the US Intelligence Community', 13 February 2018, 5, https://perma.cc/2J27-8AE5.
[35] Rogers quoted in: Blake, 'Analysis: NSA Director Mike Rogers's Remarkable Comments about Trump's Russia Efforts — or Lack Thereof'.
[36] McMaster cited in: Ryan Browne, 'McMaster: "We Have Failed to Impose Sufficient Costs" on Russia', CNN, 4 April 2018, https://www.cnn.com/2018/04/03/politics/mcmaster-russia-costs/index.html.
[37] White House, 'Statement from the Press Secretary', 15 February 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
[38] Bossert cited in: Andy Greenberg, 'The Untold Story of NotPetya, The Most Devastating Cyberattack in History', *Wired Magazine*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

including Maersk, FedEx, and Merck, and inflicting over 10 billion dollars' worth of damage.[39] Maersk's shipping terminal in Elizabeth, New Jersey, along with seventeen other Maersk terminals globally, were brought to a standstill for days.[40] At Merck, a pharmaceutical company, 15,000 Windows machines were destroyed in 90 seconds.[41] According to the US Treasury, the attack "significantly disrupted global shipping, trade, and the production of medicines. Additionally, several hospitals in the United States were unable to create electronic records for more than a week."[42] NotPetya thus harmed US economic interests and possibly even impacted the medical care of US citizens.

The response of the United States and allied countries was to first publicly attribute the attack to the Russian GRU, the military intelligence service, and, secondly, to impose a blanket sanctions package for a range of Russian cyber misdemeanours. Of the nineteen individuals sanctioned, the vast majority had no involvement in NotPetya; for example, twelve were from the infamous Internet Research Agency, which was responsible for disinformation campaigns ahead of the 2016 election.[43] Six senior members of the GRU were also named, with all but two having been sanctioned by the Obama administration previously.[44] The public attribution of the operation also bore little cost for Russia. Unlike the United States, which cares a great deal about the stealth of its offensive cyber activities, Russia has historically been comfortable with the "implausible deniability" of its operations and their public exposure, a feature it shares with other authoritarian states.[45] Public attribution, according to Chris Painter, the US Coordinator for Cyber Issues until August 2017, was "less effective against Russia and North Korea because they don't care. It's almost a badge of honour sometimes."[46]

There is little doubt that the operations described above created significant effects for national security. Scholars have already shown that cumulatively cyber operations can affect sources of national power because they undermine economic competitiveness, military advantages, and political cohesion.[47] Indeed, one of the major features of the "virtual weapon," as Kello put it, is that it "enables

---

[39] Greenberg.
[40] Greenberg.
[41] Andy Greenberg, 'How the Worst Cyberattack in History Hit American Hospitals', *Slate Magazine,* 5 November 2019, https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html.
[42] U.S. Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks', 15 March 2018, https://home.treasury.gov/news/press-releases/sm0312.
[43] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), 243.
[44] U.S. Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks'; Greenberg, *Sandworm*, 243.
[45] Buchanan, *The Hacker and the State*, 305.
[46] Painter also emphasised the necessity of responding in a publicly visible way: "Going to the NotPetya or WannaCry example: just saying 'there will be consequences' and then there's nothing else … you need to see something, right? You're not going to see everything, certainly. But having at least something seen, I think, is really important. To say: we are holding those people accountable." Author interview with Christopher Painter, 31 August 2020.
[47] Richard J. Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies*, 4 March 2020, 2, https://doi.org/10.1080/01402390.2020.1732354; Emily Goldman, 'From Reaction to

new forms of strategic effect that do not involve violence."[48] The destructive and disruptive effects of hostile cyber operations were also recognised by both administrations. Already in 2015, the Obama White House announced that it would respond to "harms caused by significant malicious cyber-enabled activities," which included, most notably, "[s]ignificantly disrupting the availability of a computer or a network of computers, including through a distributed-denial-of-service attack."[49] The Trump administration, similarly recognising the extensive damage to US national interests wrought by cyber attacks, set as its objective a "significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force."[50]

All the interviewees for this case study expressed the view that the attacks hitting the United States harmed national security interests and that the weak US responses did little to dissuade adversaries from further attacks. James Miller, the former Under Secretary of Defence for Policy, said that during his time in the Obama administration he had been conscious of the need to "hit back" for cyber attacks because the failure to do so "basically means you're saying it's OK."[51] Gary Corn, who served as Cyber Command's General Counsel both under the Obama and Trump administrations, explained that "inaction, passivity, is a counter-deterrent. It encourages. And that's what we're seeing."[52] He further elaborated that America's "reticence to respond" to cyber attacks meant that "the incentives [for adversaries] for engaging in malicious cyber activity are so much higher than the risks and costs."[53] James Clapper, the Director of National Intelligence from 2010 to 2017, noted that: "[u]ntil such time as we do create both the substance and the mindset of deterrence, this sort of thing [hostile cyber activity] is going to continue."[54] The aforementioned leaked NSA correspondence also revealed that as far back as 2013 the NSA was concerned about adversaries developing sophisticated capabilities and launching more damaging attacks against the United States.[55] In light of policymakers' recognition that the attacks were harmful to US national security interests and the failure to retaliate would invite further attacks, the question that arises is: why were the punitive responses so weak?

The answer, this thesis argues, lies in the risk society: the risk paradigm operating within policy circles informed policymakers' decision-making calculus at the time of the responses in such a way as to heighten their sensitivity to the uncertainties of the cyber operational environment, leading them to

---

Action: Adopting a Competitive Posture in Cyber Diplomacy', *Texas National Security Review* 3, no. 4 (Fall 2020): 84–101.

[48] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 196.

[49] Daniel, 'Our Latest Tool to Combat Cyber Attacks'.

[50] Office of the Coordinator for Cyber Issues, 'Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats' (U.S. Department of State, 31 May 2018), https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

[51] Author interview with James Miller, 20 August 2020.

[52] Author interview with Gary Corn, 13 August 2020.

[53] Author interview with Gary Corn.

[54] Clapper quoted in: Kello, *The Virtual Weapon and International Order*, 206.

[55] National Security Agency, 'Iran - Current Topics, Interaction with GCHQ'.

conclude that they were unwilling to accept the risks of a meaningful punishment (the risk of misattribution and the risk of unintended effects, particularly escalation), resulting in the adoption of weak, delayed responses such as public attributions, sanctions, or criminal indictments. The lens of risk, to use Mikkel Vedby Rasmussen's concept, became their "form of rationality."[56]

4.3 The birth of the US risk society

As Chapter 2 noted, states high on the risk spectrum are characterised by three primary, related features: reflexivity, preoccupation with risks (potential disastrous scenarios), and proactiveness in the employment of preventive measures and/or paralysis in a situation of response. The extent to which a state becomes a risk society is, according to Beck, strongly linked to "the history and symbols of one's culture" – or what he called "the social fabric of knowledge."[57] This section will use the risk society literature and "war as risk management" literature to discuss the roots of the US risk society – how increased reflexivity, changing American perceptions of risk, and a growing preference for pre-emptive action were influenced by socio-cultural contexts and historical events.

Let us explore the three primary forces, societal, historical, and cultural, in turn. The first factor – societal changes – were the result of an increased societal awareness of the negative side effects of industrialisation, modernisation, and globalisation, which generated a widespread anxiety about future disaster scenarios (increased reflexivity).[58] As Beck noted, "through our past decisions about atomic energy and our present decisions about the use of genetic technology, human genetics, nanotechnology, and computer science, we unleash unforeseeable, uncontrollable, indeed even *incommunicable* consequences that threaten life on earth."[59] Events such as the 1986 Chernobyl disaster became a stark reminder for highly industrialised countries like the United States that societal progress is not linear and modernisation holds negative consequences for human health and the environment.[60] For a society to become aware of these potential dangers, it required a high level of education – thus, Beck and Giddens observed, there was a close link between the growth in knowledge and the increased societal sense of risk.[61] This consciousness of unintended side effects of modernisation within risk societies contrasted sharply with the "normative project" of industrial society, which prioritised equality and the elimination of scarcity through the production and distribution of goods.[62]

---

[56] Mikkel Vedby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century* (Cambridge: Cambridge University Press, 2006), 5.
[57] Ulrich Beck, *World Risk Society* (Cambridge: Polity, 1999), 143.
[58] Beck, 143.
[59] Ulrich Beck, 'The Silence of Words: On Terror and War', *Security Dialogue* 34, no. 3 (1 September 2003): 257, https://doi.org/10.1177/09670106030343002.
[60] Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006), 34.
[61] Beck and Giddens referenced in: Frank Furedi, 'Precautionary Culture and the Rise of Possibilistic Risk Assessment', *Erasmus Law Review* 2, no. 2 (November 2009): 201.
[62] Heng, *War as Risk Management*, 2006, 34.

Further compounding social anxiety in the United States was the fact that, according to Frank Furedi, "Western societies possess[ed] a weak sense of shared meaning and therefore often lack[ed] a consensus about how to attribute blame and responsibility." As a result, "the link between cause and negative outcome [has been] continually contested." The confusion about cause and effect, argued Furedi, further fuelled the perception that disastrous events were "incomprehensible and beyond human control."[63]

One manifestation of societal anxiety about the unknown side effects of industrialisation was the emergence and growth in popularity in the United States of the "precautionary principle," first in the context of climate change and later with regard to broader issues of national security. The most widely known definition of the principle comes from the 1992 Rio Declaration on Environment and Development: "[w]here there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."[64] The precautionary principle was seen to offer a potential solution to what Beck called "the risk trap": a situation in which there is a significant gap in knowledge but nevertheless decisions have to be made.[65] More problematically, the principle was later often applied as part of the justification of pre-emptive or anticipatory military action, in situations where there was "a lack of evidence of harm or straightforward causal relationships."[66] The application of the principle thus expanded from issues of scientific uncertainty to major political and strategic decisions such as the US decision to invade Iraq in the early 2000s.[67] In this way, argued Heng, the precautionary principle became a "culturally framed concept," "incorporating non-scientific public opinion and social values."[68] As the debate between the United States and certain European countries on the war in Iraq showed, while the principle purports to be universal, the precautions that one state may regard as reasonable may be completely unreasonable to another.[69] The growth in the use of the precautionary principle in the United States was thus a symptom of a much deeper "disillusionment with progress"[70] and a general "culture of fear" where "every conceivable experience ha[d] been transformed into a risk to be managed."[71]

---

[63] Furedi, 'Precautionary Culture and the Rise of Possibilistic Risk Assessment', 201.
[64] European Commission et al., 'The Precautionary Principle: Decision-Making under Uncertainty.', Science for Environment Policy (Brussels, Belgium: European Commission, September 2017), 3, http://data.europa.eu/doi/10.2779/709033.
[65] Heng, *War as Risk Management*, 2006, 55.
[66] European Commission et al., 'The Precautionary Principle', 8; Heng, *War as Risk Management*, 2006, 56.
[67] Heng, *War as Risk Management*, 2006, 56.
[68] Heng, 56.
[69] Coker, *War in an Age of Risk*, 101.
[70] Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006), 153.
[71] Furedi, 'Precautionary Culture and the Rise of Possibilistic Risk Assessment', 200.

Why was the United States particularly susceptible to societal anxieties about risk, especially in relation to some other highly industrialised countries?[72] In addition to the population's high level of education and the country's unmatched technological development, central to the emergence of the US risk society was the country's historical experience. The war as risk management literature places particularly strong emphasis on how the United States was left searching for a new ideological challenger and adversary in the 1990s after the collapse of the Soviet Union. During the Cold War, strategic thinking had revolved around the survival threat posed by a nuclear superpower; that environment had held far more certainty for the United States than the post-Cold War environment.[73] Policymakers had known who their adversary was (the Soviet Union), what their intention was (the spread of communist ideology), and their potential to inflict damage (possession of conventional military and nuclear weapons).[74] The ability to link a security issue to a single, ideologically-opposed actor with quantifiable arms meant that these issues were perceived as threats rather than risks.[75] The 1982 National Security Strategy, for example, was entirely focused on the USSR as a military threat: its priorities included deterring a Soviet attack, strengthening western alliances against the Soviet threat, "containment" of Soviet expansionism, and limiting Soviet military capabilities and alliances.[76]

The end of the "East-West conflict," coupled with the revolution in information technology, fundamentally changed security and intervention policy under President Bill Clinton and accelerated the fragmentation of traditional power structures.[77] Lacking the "historical purpose" of the Cold War, Heng showed that the United States under Clinton gradually became less willing to make sacrifices for solving global security problems (despite being militarily pre-eminent) as these were becoming less clearly defined and more transnational in nature. They included issues like ethnic conflict, infectious diseases, economic collapse, weapons proliferation, drug trafficking, terrorism, and transnational crime and could not be handled using familiar strategies of deterrence.[78]

Under the subsequent administration of George W. Bush, the terrorist attacks of September 11th 2001 focused attention squarely on transnational terrorism and rogue actors.[79] This period marked the intensification of the culture of political anxiety and increased sensitivity to risk, especially because the

[72] The United States is not alone in its risk sensitivity. Another country that has been extensively examined by the sociologists as a risk society is the United Kingdom. See for example: Anthony Giddens, 'Risk Society: The Context of British Politics', in *The Politics of Risk Society*, ed. Jane Franklin (Cambridge: Polity Press, 1998).
[73] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London; New York: Routledge, 2010), 19; Deborah D. Avant, 'Are the Reluctant Warriors out of Control? Why the U.S. Military Is Averse to Responding to Post-cold War Low-level Threats', *Security Studies* 6, no. 2 (December 1996): 51, https://doi.org/10.1080/09636419608429306.
[74] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 19.
[75] Williams, 18.
[76] The White House, 'U.S. National Security Strategy', Federation of American Scientists, 20 May 1982, 1–3, https://fas.org/irp/offdocs/nsdd/nsdd-32.pdf.
[77] Alexander Wolf, 'US Interventions Abroad: A Renaissance of the Powell Doctrine?', *Strategic Studies Quarterly* 3, no. 4 (2009): 128.
[78] Heng, *War as Risk Management*, 2006, 21–24.
[79] Heng, 24.

events of 9/11, according to Coker, reminded Americans of the "stealth" attack of 1941, which had drawn the United States into the Second World War.[80] The new National Security Strategy of 2002 formally announced the abandonment of a "reactive posture" in favour of "anticipatory action … even if uncertainty remains as to the time and place of the enemy's attack."[81] The Strategy explained that such a change in strategic posture was necessary because the "leaders of rogue states [were] more willing to take risks" than the United States.[82] The new strategy thus formally adopted the precautionary principle to address the risk of terrorism and the guiding maxim of the Bush era became "prevention is better than punishment."[83] Encapsulating the atmosphere after 9/11, Tom Ridge, then Director of US Homeland Security, explained that in matters of national security "[t]here is [now] a universe of potentials we have to deal with."[84] The Bush administration's military engagements in Afghanistan and Iraq subsequently therefore became proactive exercises in risk management.[85]

The risk sensitivity from 9/11 continued to dominate societal perceptions under the Obama administration. Drones offered a particularly attractive option for "controlling the apportionment of risk" and indeed Obama became well-known for managing the risks of transnational terrorism through the use of unmanned aerial vehicles (UAVs) and special operations raids.[86] The sense of insecurity was also not limited to policymakers. As the risk sociologists described, perceptions of risk are a culturally informed "collective construct."[87] In a 2009 Pew survey, 58% of the US general public believed the world was more dangerous for the United States than during the Cold War and the majority supported the use of pre-emptive force.[88] Robert Jervis wrote in 2011 that "[i]f through effort or good fortune the problem we worry most about disappears, all the others move up a notch … We are now so worried about terrorism because our security environment is otherwise so benign. The fact that we no longer have to live under the shadow of instantaneous destruction has much less impact on our psyches and sense of how dangerous our world is than logic would suggest."[89]

---

[80] Coker, *War in an Age of Risk*, 101.
[81] The White House, 'The National Security Strategy of the United States of America', September 2002, 15, https://2009-2017.state.gov/documents/organization/63562.pdf.
[82] The White House, 15.
[83] Jessica Stern and Jonathan B. Wiener, 'Precaution Against Terrorism', *Journal of Risk Research* 9, no. 4 (1 June 2006): 394, https://doi.org/10.1080/13669870600715750; Coker, *War in an Age of Risk*, 140.
[84] Ridge quoted in: Christopher Coker, *Globalisation and Insecurity in the Twenty-First Century: NATO and the Management of Risk*, Adelphi Papers ; No. 345 (Oxford and New York: Oxford University Press for the International Institute for Strategic Studies, 2002), 62.
[85] Heng, *War as Risk Management*, 2006.
[86] Heng, 548–50.
[87] Mary Douglas and Aaron B. Wildavsky, *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers* (Berkeley: University of California Press, 1982), 79–80.
[88] Pew Research Center, 'Section 2: Global Threats and Use of Military Force' (Washington, D.C.: Pew Research Center, 3 December 2009), https://www.pewresearch.org/politics/2009/12/03/section-2-global-threats-and-use-of-military-force/.
[89] Robert Jervis, 'Pinker the Prophet', ed. Steven Pinker, *The National Interest*, no. 116 (December 2011): 57. Other scholars made similar points, for example: Dominic D.P. Johnson and Dominic Tierney, 'Bad World: The Negativity Bias in International Politics', *International Security* 43, no. 3 (1 February 2019): 104, https://doi.org/10.1162/isec_a_00336; Heng, *War as Risk Management*, 2006, 154; Rasmussen, *The Risk Society at War*, 1.

Nor did risk sensitivity wane in later years. In a 2018 paper, Heng took the concepts he had applied to the "risk management wars" of the early 2000s and sought to use them to elucidate American and British military operations in Libya, Islamic State, Syria, Niger, Yemen, and Somalia. He found that, despite the fact that the strategic context in 2018 differed markedly from that in the 2000s, risk management, as opposed to considerations of imminent survival threats, was still the predominant logic shaping deliberations on war.[90] Analysing decision-making under the Trump administration in relation to disrupting terror networks in Afghanistan, Heng detected the employment of "minimalist risk management goals," rather than grander aims such as nation-building. He noted that this "minimalist utilitarian calculus" was grounded in an appreciation of the fact that risks cannot be completely eliminated, only managed.[91]

Alongside 9/11 and transnational terrorism, the digital revolution became another propellant of risk sensitivity. Anxiety about the uncertainties and potential for surprise inherent in computer-born hazards was palpable in almost every US policy discussion on the subject. Early on, the potential for a "cyber Pearl Harbour," put forward in a 2012 speech by Defence Secretary Leon Panetta, generated particular angst among policymakers and the general population.[92] As former US Secretary of Defense Chuck Hagel pointed out in 2014, "America has always adapted to new threats. But today, a networked world – a world in which oceans are crossed at the speed of light – presents challenges to American security that our nation has never before confronted."[93] Henry Kissinger, reflecting on the differences between the "new [technological] age" and the Cold War commented that, "[i]t is far more complex … And over the long term, it may be far more dangerous."[94] According to President Obama, "cyberspace is real. And so are the risks that come with it." Demonstrating the reflexivity that characterises risk societies, he continued: "[i]t's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy."[95]

What this short journey through the United States' historical trajectory illustrates is that, from the collapse of an ideological challenger, through becoming a victim of transnational terrorism, to the experience of a digital technological revolution, historical events and transformations have played a key role in fostering the emergence of the US risk society.

---

[90] Yee-Kuang Heng, 'The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions', *Contemporary Security Policy* 39, no. 4 (2 October 2018): 545–48, https://doi.org/10.1080/13523260.2018.1494670.
[91] Heng, 552.
[92] As Panetta later revealed in an interview with journalist David Sanger, he had intentionally used the evocative analogy in order to "get Congress to focus on the issue." See: U.S. Department of Defense, 'Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', 11 October 2012, https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136; Sanger, *The Perfect Weapon*, 162.
[93] Hagel cited in: U.S. Department of Defense, 'Secretary of Defense Speech: Retirement Ceremony for General Keith Alexander', 28 March 2014, https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1837.
[94] Kissinger cited in: Sanger, *The Perfect Weapon*, xxiii.
[95] Obama's transcribed speech in: The New York Times, 'Text: Obama's Remarks on Cyber-Security', *The New York Times*, 29 May 2009, sec. U.S., https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html.

The third force contributing to the risk society have been cultural factors, or more specifically, American strategic culture. The notion that strategic decision-making and behaviour is a cultural exercise is no longer new; the concept of "strategic culture" has generated a particularly rich subset of scholarship within security studies.[96] Fundamentally, the guiding belief in the United States is that warfare is an "aberration in human relations" because "[m]an can pursue his productive pursuits, and maximize his values only in the absence of war."[97] Thus, the US "ideology on participation in war" is premised on the idea that the United States should only go to war in pursuit of "good," or "just," causes.[98]

Relatedly, a value system that "accords great importance to the well-being of individuals" and human rights more generally, translates into casualty aversion in conflict.[99] Prioritising force protection, US commanders prefer a high-technology approach to war, with as much reliance on machines as possible.[100] Sapolsky and Shapiro argued that pride in military superiority and the military presenting itself as a vehicle for social mobility were a particular source of high sensitivity to soldier casualties.[101] This sensitivity was manifestly on display when Clinton decided to rapidly withdraw US forces from Somalia in 1993, for example.[102]

The US aversion to casualties is not limited to its own soldiers – it also extends to the adversary's civilian population. Coker argued that much of the American attention to protecting human life in war can also be traced back to horrific televised images of civilian casualties during the Vietnam war.[103] The United States, he wrote, is "haunted by a bad conscience: by the memory of what it did in the past in the name of its former unquestioning belief in reason, civilisation, or progress."[104] This is why now "the individual has been placed at the centre of the moral imagination."[105] According to Coker, as a result of these social, historical, and cultural factors, American strategic thinking has become inherently risk-averse – something that, he argued, US adversaries are acutely aware of.[106]

---

[96] Ken Booth, 'The Concept of Strategic Culture Affirmed', in *Strategic Power: USA/USSR*, ed. C. G. Jacobsen et al. (Basingstoke: Macmillan, 1990), 121.
[97] Alastair Iain Johnston, 'Thinking about Strategic Culture', *International Security* 19, no. 4 (1995): 32, 39, https://doi.org/10.2307/2539119.
[98] Colin S. Gray, 'National Style in Strategy: The American Example', *International Security* 6, no. 2 (1981): 26, https://doi.org/10.2307/2538645.
[99] Gray, 38.
[100] Colin S. Gray, 'Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?' (Carlisle, PA: Strategic Studies Institute, US Army War College, 2006), 49, https://hdl.handle.net/2027/mdp.39015063246428.
[101] Harvey M. Sapolsky and Jeremy Shapiro, 'Casualties, Technology, and America's Future Wars', *Parameters; Carlisle Barracks, Pa.* 26, no. 2 (Summer 1996): 124.
[102] Simon Tisdall, 'Mogadishu Outrage Puts Clinton in Firing Line', *The Guardian*, 5 October 1993, http://www.theguardian.com/world/1993/oct/05/usa.simontisdall1.
[103] Christopher Coker, *Humane Warfare* (London ; New York: Routledge, 2001), 37.
[104] Coker, 42.
[105] Coker, 18.
[106] Christopher Coker, *Waging War without Warriors?: The Changing Culture of Military Conflict* (London: Lynne Rienner Publishers, 2002), 64.

While cyber conflict has not yet reached a level of intensity that would result in casualties, the cultural underpinnings of American risk aversion in war are also manifested in the cyber domain. As this chapter will later elaborate, US decision-makers are particularly attuned to the potential unintended effects of cyber response actions as, given the interconnectedness of cyberspace, any unintended effects of an offensive cyber operation are highly likely to impact civilian infrastructures, potentially resulting in civilian harm or disruption to everyday life.

More broadly, the societal dispositions, historical experiences, and cultural inclinations of the United States described above mean that, with regard to the cyber domain, US policy is made with a particular focus on the features of cyberspace that make it a domain prone to uncertainty and surprise outcomes. This has led to, on the one hand, paralysis in responding to individual damaging cyber operations, as a result of "playing out every worst-case scenario,"[107] and, on the other, a strong preference for preventive practices to mitigate the risk of perceived future worst-case scenarios. Although the United States' main geopolitical adversaries (Russia, China, Iran, and North Korea) are well-known, the difficulty of determining the extent of their cyber capabilities and the intent of their operations at any one time means that in the cyber realm, conflict with many and diverse geopolitical competitors is perceived to be even more riddled with uncertainty than in other operational domains. The next section will turn to examining these dynamics in more detail.

4.4 The rejection of meaningful response: the risk society (in)action

As Chapter 2 and Chapter 3 outlined, risk societies are continually preoccupied with trying to control and manage uncertainties.[108] They worry about the fact that contemporary hazards cannot always be anticipated "by applying the usual rules of cause and effect" because "many are unintended."[109] In cases where there is high uncertainty as to the potential consequences of actions, risk societies are likely to invoke worst-case scenarios and experience decision paralysis. To what extent can the risk society framework explain the decisions made by the United States in terms of its responses to cyber attacks? And does the risk society shed light on why US responses were not timely or severe enough to attempt to deter further attacks?

The following sections will show that, aligning with the expectations of the risk framework, US policymakers exhibited a particular concern with the operational characteristics of the cyber domain that most contribute to the creation of uncertainty in the context of responding to cyber attacks: the nature of cyberspace as a complex system and the ease of proliferation of cyber capabilities. Moreover,

---

[107] Ilan Goldenberg et al., 'Countering Iran in the Gray Zone: What the United States Should Learn from Israel's Operations in Syria' (Center for a New American Security, 2020), 12, https://www.jstor.org/stable/resrep24223.7.
[108] Coker, *War in an Age of Risk*, 76.
[109] Coker, 70.

the risks that these create, namely the risk of misattribution and the risk of unintended effects (particularly escalation) will be shown to have posed obstacles to meaningful punishment in all the cases of cyber incidents examined above.

4.4.1 Concerns about the cyber operational environment: proliferation and complex adaptiveness

During the Obama administration, the concern about the proliferation of cyber capabilities, its empowerment of otherwise weaker actors, and the potential for worst-case scenarios arising from the complexity and interdependence of cyberspace, was visible at the highest levels of US government. "In a future conflict", wrote Obama in an op-ed, "an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities at home. Taking down vital banking systems *could trigger a financial crisis*. The lack of clean water or functioning hospitals *could spark a public health emergency* [emphasis added]."[110] Obama's Secretary of Defense, Chuck Hagel, cautioned: "[o]ur nation confronts the proliferation of destructive malware and a new reality of steady, ongoing and aggressive efforts to probe, access, or disrupt public and private networks, and the industrial control systems that manage our water and our energy and food supplies."[111] Hagel's advisor, Under Secretary of Defense for Policy James Miller, added that the "potential for [adversaries] reverse-engineering malware used in a response" and the chance of "spill-over effects" (the possibility that malware might spread outside its intended target because the Internet is a "complex system of systems and there can be emergent behaviour") were crucial considerations when devising responses.[112]

US policymakers felt their country was asymmetrically vulnerable because of the cyber domain's empowerment of militarily weaker actors and the United States' enormous dependence on cyber technologies. Michael Daniel, Cybersecurity Coordinator on the National Security Council during the Obama administration, recalled that "we always felt like we lived in a glass house" because "we were one of the most digitally-dependent nations around."[113]

The awareness of the cyber domain's technical features, and the realisation that adversaries were using these to their advantage, led policymakers under the Trump administration to develop an understanding of the cyber domain as an "environment of constant contact," a concept which was first proposed by Richard Harknett and Director of the US Cyber Command/ NSA Combined Action Group, Emily Goldman, in 2016.[114] In their view, which became highly influential in the Department of

[110] Barack Obama, 'Op-Ed by President Obama: Taking the Cyberattack Threat Seriously', 19 July 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously.
[111] Hagel cited in: U.S. Department of Defense, 'Secretary of Defense Speech: Retirement Ceremony for General Keith Alexander'.
[112] Author interview with James Miller.
[113] Author interview with Michael Daniel, 10 September 2020.
[114] Richard J. Harknett and Emily Goldman, 'The Search for Cyber Fundamentals', *Journal of Information Warfare* 15, no. 2 (2016): 86.

Defense (DoD) and in Cyber Command,[115] it was the cyber domain's high level of complexity and interconnectedness which meant that "the defense is in *constant contact* with the enemy."[116]

The 2018 Cyber Command (CYBERCOM) Vision Document was one of the first documents that emerged from these new conceptual clarifications. Paying particular attention to the uncertainties inherent in cyberspace, the document explained the DoD's perception of the domain as "a fluid environment of constant contact and shifting terrain. New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent." In characteristic risk society fashion, the description ended with: "[w]ell-defended cyber terrain is attainable but *continually at risk* [emphasis added]."[117]

Key policymakers also worried about the ease of proliferation of capabilities and the diversity of actors in the cyber domain (operational characteristic 2). General Paul Nakasone, Commander of US CYBERCOM and Director of NSA under the Trump administration, explained that, "[threats in cyberspace] persist because the barriers to entry are low and the capabilities are rapidly available and can be easily repurposed."[118] Goldman also referred to the domain's complex adaptiveness (operational characteristic 1) and the challenge of attribution (consequence 1): "[the cyber domain] is globally interconnected, distinguished by constant (rather than imminent, potential, or episodic) contact, influenced by difficulty of attribution."[119]

What these excerpts and quotes show us is that both under the Obama administrations and under the Trump administration, in accordance with the risk framework, policymakers were strongly preoccupied with the domain's operational characteristics, particularly its complexity and the ease of proliferation of cyber capabilities, which, as Chapter 3 explained, lie at the source of the domain's inherent uncertainty and pose a particular challenge for risk societies. Nor did the attention that policymakers devoted to these operational characteristics wane over time. In a speech in October 2020, Trump's Assistant Secretary for International Security and Nonproliferation, Christopher Ford, highlighted that "effective risk reduction in the cyber domain is challenged by several important characteristics," including the difficulty of attribution, the "ubiquity and often dual use nature" of cyber capabilities, and their "possession by both state and non-state actors," which makes "cyberspace tools

---

[115] Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* 5, no. 1 (1 January 2019): 5, https://doi.org/10.1093/cybsec/tyz008.
[116] Harknett and Smeets, 'Cyber Campaigns and Strategic Outcomes', 2. Constant contact also signified that it was impossible to completely eliminate risks in cyberspace. Instead, as a result of this new understanding, like the risk framework anticipated, the United States ramped up risk management practices, particularly preventive action. These came in 2018 in the form of the strategies of defend forward and persistent engagement (DF and PE), which will be explored in detail in section 4.5 as part of the discussion of risk management.
[117] U.S. Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command' (United States Cyber Command, 2018), 4, https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.
[118] Paul M. Nakasone, 'An Interview with Paul M. Nakasone', *Joint Force Quarterly*, no. 92 (January 2019): 4.
[119] Goldman, 'From Reaction to Action'.

difficult to define or control." Ford also noted that, for the same reasons, effective arms control in cyberspace is impossible, presenting a problem for estimating the capabilities of adversaries.[120] As the risk framework specified, for risk societies, the inability to calculate adversaries' cyber capabilities will be conducive to imagining worst-case scenarios.

Having discussed policymakers' concerns about the domain's operational characteristics, we now move on to looking at their consequences: the risks of misattribution and the risk of unintended effects. The following two subsections will show how, as per the expectations of the risk framework, the risk of misattribution and plausible deniability and risk of unintended effects became significant obstacles for issuing meaningful punishments.

4.4.2 Concerns about the risk of misattribution and plausible deniability

Chapter 3 discussed how the complexity of the cyber operational environment and the proliferation of capabilities make the process of attributing cyber attacks longer and more difficult. The risk framework expected that, because of risk societies' aversion to uncertainty, they would be unwilling to tolerate the risks of misattribution or plausible deniability in return for a timely response. In other words, risk societies would not be comfortable issuing a response without first having achieved what they perceive to be high levels of confidence in the identification of the perpetrator. This is problematic because, as Chapter 1 explained, one of the crucial elements of a meaningful punishment is swiftness.

Bob Butler, former Deputy Assistant Secretary of Defense under the Obama administration, explained that "[w]hen I last served full-time in the US federal government, the issue of attribution often dominated our conversations when discussing cyberattacks against US interests. Positive attribution was a key foundation and often a pacing activity for taking response action. Because of the challenges in this area of attribution, formulation and execution of appropriate responses actions took time."[121] Chris Inglis, former Deputy Director of the NSA, noted that public attribution statements always needed to be justified with evidence, which, like the risk framework outlined, raised problems in terms of disclosing the confidential sources and methods that led a government to its conclusions.[122] Policymakers were also acutely aware that the longer they took to attribute an operation, the more this would interfere with what Schelling called "the idiom of reprisal."[123] "When there is a lag time in attribution," Gary Corn affirmed, "the urgency of response dissipates."[124] Yet, the US government was

[120] U.S. Department of State, 'Responding to Modern Cyber Threats with Diplomacy and Deterrence: Remarks Dr Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Center for Strategic and International Studies, Washington DC', United States Department of State, 19 October 2020, https://2017-2021.state.gov/responding-to-modern-cyber-threats-with-diplomacy-and-deterrence/index.html.
[121] Author interview with Bob Butler, 3 September 2020.
[122] Author interview with Chris Inglis.
[123] Schelling, *Arms and Influence*, 141–45.
[124] Author interview with Gary Corn.

unwilling to accept the risks of potentially misattributing an attack in order to issue a timely punishment – according to Miller, attributing an attack to the wrong party would "undermine the credibility of the United States" and risk undermining the support of allies in a future scenario.[125]

The case of NotPetya, which occurred during the Trump administration, demonstrates how a lengthy attribution process impeded a meaningful response. The United States issued a statement, which it coordinated with allies (specifically the UK, Denmark, Lithuania, Estonia, Canada, and Australia), attributing NotPetya to Russia in February 2018.[126] The choice of collective attribution was selected in order to make the statement more credible.[127] From a risk society perspective this is not surprising as collective attribution *decreases* the perceived risks of misattribution – in theory, this means that the judgement was reached on the basis of shared intelligence, and therefore more evidence, thus increasing the level of confidence in it and lessening the risk of the adversary plausibly denying their culpability.

NotPetya also illustrates how a delayed attribution, as a result of the need for the US risk society to achieve high confidence in the judgement and communicate it publicly prior to issuing a response, interfered with the imposition of meaningful penalties. The attribution statement was released more than seven months after the operation had taken place.[128] The enormous delay in publicly attributing NotPetya meant that other events came to pass in the interim, resulting in the punishment of NotPetya no longer being a high priority on policymakers' agendas or at the forefront of public attention. The day after the White House publicly attributed the operation to Russia on February 15th 2018, the US Justice Department issued a momentous indictment of 13 Russian officials and three companies, including the Internet Research Agency, for interfering in the 2016 presidential election.[129] The indictment and the revelation of a sweeping Russian disinformation campaign dominated headlines and consumed the attention of the public as well as policymakers.[130] Thus, when the US Treasury announced a sanctions package in March 2018, it became apparent that the sanctions did not punish NotPetya specifically, but instead were a response to a whole host of different Russian cyber activity, "ranging from interference in the 2016 US elections to conducting destructive cyber-attacks, including the NotPetya attack."[131] In addition to sanctioning the Russian Federal Security Service and Main Intelligence Directorate as well

[125] Author interview with James Miller.
[126] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (London: Hurst & Company, 2016), 304.
[127] Author interview with Anonymous US State Department Official, 8 October 2020; Author interview with Emily Goldman, 1 September 2020.
[128] Buchanan, *The Cybersecurity Dilemma*, 304.
[129] Department of Justice, 'Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities'.
[130] Matt Apuzzo and Sharon LaFraniere, '13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign', *The New York Times*, 16 February 2018, sec. U.S., https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.
[131] U.S. Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks', 15 March 2018, https://home.treasury.gov/news/press-releases/sm0312.

as six individuals for broad cyber-enabled activity, which included NotPetya, the Treasury sanctioned a different set of entities and individuals, those that had been listed in Special Counsel Mueller's indictment (including the Internet Research Agency), for a different set of effects, namely election interference.[132]

The connection between the act and the response, so crucial for meaningful punishment, was therefore heavily muddied by events that occurred in the interim. And although the US Treasury referred to NotPetya in announcing the sanctions, the long list of Russian misdemeanours included in the same press release significantly diluted its meaning. What's more, the intent behind NotPetya to this day remains ambiguous, while the intent behind the election campaign was clearly stated in the indictment as being the undermining of trust in the US political system.[133] An attempt to punish general "malign Russian cyber activity" in one action and the lack of differentiation between the attacks, seemed to signal to Russia that it was being punished on the basis of the *means* employed in the attacks, rather than for the *intent* behind the operations or their *effects*. Having not differentiated between operations, the response to Russia's cyber activities, including NotPetya, was therefore unlikely to have given the adversary, in Schelling's words, "a basis for judging what to expect as the consequences of his own actions."[134] As Chris Painter noted, "[if] you say that there is going to be something and then it doesn't end up happening right when you say it, and then it's mushed together with a whole lot of other things – Russian misconduct writ large – it's very difficult to see how that's going to change behaviour."[135]

We can conclude therefore that not only did the United States behave in accordance with the expectation of the risk framework in wanting to achieve high confidence in attribution prior to issuing a punishment, but we also see how in its quest to minimise the risk of misattribution and plausible deniability, the United States found itself in a situation where the imposition of meaningful costs for NotPetya, that would deter Russia from future such attacks, was no longer viable.

What is more, the US choice of criminal indictments over other, punchier forms of response coheres with the objective of risk avoidance. This is because criminal charges require a higher burden of proof than standards of information that typically form the basis for national security decision-making; prosecutors must be prepared to prove "beyond a reasonable doubt" that a party is guilty before an independent judge and jury.[136] Striving to avoid uncertainty in attribution, in the midst of knowledge of the difficulties of this due to the complexity and anonymity granted by the operational environment, issuing indictments is a procedural way of addressing the potential risks that would result from

[132] U.S. Department of the Treasury.
[133] The United States Department of Justice, 'Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System', 16 February 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.
[134] Schelling, *Arms and Influence*, 149.
[135] Author interview with Christopher Painter.
[136] Garrett Hinck and Tim Maurer, 'Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity', *Journal of National Security Law and Policy* 10, no. 3 (January 2020): 529.

misattribution. Indictments also communicate a high level of confidence in the attribution judgement to the adversary, thus decreasing the risk that the adversary will be able to credibly rebuff the statement. As section 4.2 discussed, policymakers were fully aware that attribution statements and indictments would be ineffective in changing the behaviour of adversaries. Yet, as we can see from the NotPetya case, the desire to minimise uncertainty and risk meant that the quest for high confidence in attribution prevailed over the requirement for swiftness in punishment.

Let us now move on to an examination of the concerns that policymakers had about the risk of unintended effects from a meaningful response.

4.4.3 Concerns about the risk of unintended effects (collateral damage, blowback, and escalation)

The evidence gathered for this case study indicates that, in accordance with the risk framework, US policymakers were most concerned with the risks of unintended effects of a response (in the form of escalation, blowback, and collateral damage), which was the main factor that restrained the responses to cyber attacks. The interviews revealed that policymakers had a tendency to understand a meaningful response as being in the form of a cyber retaliation, rather than a cross-domain response.[137] This is unsurprising: recall from Chapter 1 Schelling's advice that in order to be meaningful, responses should be mounted in the same "currency."[138] Other scholars have also noted that a retaliation in kind is the easiest way to communicate punishment to an adversary.[139]

The perception that the United States was asymmetrically vulnerable in cyberspace, as a result of its dependence on digital infrastructures, made policymakers particularly worried about issuing a response that might spark an unwanted escalating cyber conflict. According to Butler, "[i]n reflecting about the nature of response action[s] themselves, US government decision makers consistently balanced risk in the area of imposing cost vis a vis managing further escalation. Responses were targeted to avoid second and third order effects which could result in unintended consequences and further escalation by an adversary."[140] Similarly, Corn explained that the thought process of policymakers was the following: "[i]f we're going to unleash the hounds of cyber war, good gracious, what's going to happen to us?... We need to be very cautious here about our approach because we just don't understand how we can control this."[141] Inglis also noted that policymakers tended to approach cyberspace with a sense of trepidation and were reluctant to "unleash hell in a space that can't constrain or contain that."[142]

---

[137] Later in this section we will also discuss how concerns about blowback also restrained cross-domain responses (specifically sanctions).
[138] Schelling, *Arms and Influence*, 146–47.
[139] Jacquelyn G. Schneider, 'Deterrence in and through Cyberspace', in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Erik Gartzke (Oxford: Oxford University Press, 2019), 114.
[140] Author interview with Bob Butler.
[141] Author interview with Gary Corn.
[142] Author interview with Chris Inglis.; James Miller, Undersecretary of Defense for Policy between 2012 and 2014, explained in an interview with the author that some policymakers in the early years were worried that

General Keith Alexander, at the time of his leadership of Cyber Command and the NSA, reasoned about escalation in terms of worst-case scenarios (a key indicator of risk thinking):

> … in launching [a] cyber-attack, suppose [your adversary] actually knock[s] out your stock exchange or temporarily disable[s] your banking system … Your government then feels it has to reciprocate. And we have an unpredictable chain reaction that could lead to outright war. … There is a significant probability of miscalculation in these cases – with catastrophic ramifications for everyone.[143]

The second unintended effect that was repeatedly referred to by policymakers was the risk of collateral damage that a cyber response might entail. Policymakers noted that in cyberspace, predicting the wider consequences of one's own actions or an adversary's was more difficult. Ash Carter, US Secretary of Defense from 2015 to 2017, illustrated this notion with the following example: "[i]t's things like: Are you sure that a particular action you take with an enemy's information system will only have the consequence of disrupting, let us say, an air-defense system."[144] Complicating things further, Corn pointed out, is the fact that "there is no clear military cyber pathway to target. Everything transits civilian infrastructure at some point or at some level."[145]

Policymakers saw a clear link between the characteristics of the operational environment and the risks these created in terms of collateral damage. Michael Daniel made a number of important points in his interview, highlighting the presence of "risk thinking" in US government during his tenure. He first pointed out that, in contrast to the physical domain, in the cyber domain it was much harder for policymakers to predict collateral damage. Secondly, he explicitly linked the two operational characteristics, the complexity of the system and the ease of proliferation, with a general increase in uncertainty in the cyber domain (recall that risk societies tend to equate uncertainty with risk).

> … If we to use a cyber tool, we don't quite know what the probability is that it will actually hit the target and have the effect that we want; we don't actually know if it will only do what we want it to do or what the collateral damage might be; and unlike the missile we've shot, *the bad guys can pick up the thing we've just used and turn it back on us or on someone else*. As a result, we've got a lot more uncertainty with cyber tools [emphasis added].[146]

"engaging in all this tit-for-tat stuff" even risked "ruining the Internet." See: Author interview with James Miller, 20 August 2020.

[143] Alexander cited in: Christopher Joye, 'Interview Transcript: Former Head of the NSA and Commander of the US Cyber Command, General Keith Alexander', Australian Financial Review, 7 May 2014, https://www.afr.com/technology/interview-transcript-former-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140508-itzhw.

[144] Carter cited in: Sanger, *The Perfect Weapon*, 38–39.

[145] Author interview with Gary Corn.

[146] Author interview with Michael Daniel.

James Clapper was also concerned about collateral damage as an unintended effect: "reciprocity and collateral damage in cyberspace are very difficult to control. ... the New York Stock Exchange or telecommunications in Eastern Europe or a power grid in Central America might well be taken offline. No one could predict the *unintended consequences* and potential damage such an assault might cause [emphasis added].[147]

Worries about the risk of unintended effects, including inadvertent escalation, blowback, and collateral damage, were also recounted by policymakers reflecting on the decision processes that led to response outcomes in individual cases of cyber incidents. Let us look at these in turn. In the case of the 2011-2013 Iranian DDoS attacks, initially, Clapper explained, the attitude at the National Security Council was hawkish: "[w]e had teed up a bunch of options for cyberattack against the very same players who had participated in these denial of service attacks [against the banks] … The initial instinct was: Let's attack back."[148] Concerns about unintended escalatory consequences connected to the United States' asymmetric vulnerability quickly seeped into the deliberations, however. Tim Geithner, then Secretary of the Treasury, pointed out that US banks might not be able to cope with an Iranian counter-retaliation.[149] Recalling this conversation, Clapper wrote: "I was particularly attuned to ... second and third order vulnerabilities because of a discussion at a Principals Committee meeting … about retaliating for cyber intrusions into Wall Street. … Treasury Secretary Tim Geithner … asked a simple question: 'Does anyone know what would happen if there was a serious attack on our financial institutions? Because I don't.' That ended the discussion."[150] While the United States had a preference for operations that were "precise, very limited, very surgical, legalistic," officials doubted whether its adversaries, in this case Iran, would exercise similar restraint in its counter-response. "If you attack them," Clapper surmised, "you have to anticipate a probably much … greater retaliation as a result."[151]

In a personal interview, Chris Inglis elaborated on the context of the Obama administration's concerns about unintended consequences at the time of the DDoS attacks:

> The Obama administration, understanding something in the nature of mistakes made by the Bush administration, dramatically standing into problems creating more chaos than perhaps good, I think, was very reluctant to stand into something that was not well understood, where the second and third order consequences might not be fully appreciated or laid out. And, therefore, there was a pretty high bar for the Obama administration to say: "I'll stand in and do something." Combine those two factors and you get an inherent reluctance of the US government in 2012-2013 to stand in.[152]

---

[147] James R. Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence* (New York: Penguin Random House Large Print, 2018), 534–35.
[148] Clapper quoted in: Shaun Waterman, 'Clapper: U.S. Shelved "Hack Backs" Due to Counterattack Fears', CyberScoop, 2 October 2017, https://www.cyberscoop.com/hack-back-james-clapper-iran-north-korea/.
[149] Geithner referenced in: Waterman.
[150] Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence*, 535.
[151] Clapper quoted in: Waterman, 'Clapper'.
[152] Author interview with Chris Inglis.

Particularly interesting here in the context of the risk society theory is the emphasis on "lessons learned" from the blunders of the previous administration – it illustrates Beck's point that the understanding of risk by policymakers is mediated by historical events.[153] Mindful of escalation risks, the Obama administration decided instead to engage in managing the consequences of the Iranian operation (which will be discussed in section 4.5 on risk management practices).

Around the time of the DDoS operation, concerns about potential blowback also acted as a restraint of both the United States' *own* offensive cyber operations, translating into a reluctance to use them in a reprisal, and in the application of economic sanctions for cyber attacks. One senior official explained that the discussion of whether to publicly acknowledge the United States' offensive cyber program, and the blowback this could cause, came to a head during the Iranian DDoS attacks and caused an "inter-agency fracas." Already at the start of Obama's time in office, officials had been prohibited from even using the phrase "offensive cyber" as there was a view that building an offensive cyber capabilities would "undermine global norms and support for the Internet and that could cause blowback on the US and hurt our economic interests and hurt us diplomatically."[154] On the question of economic sanctions, Michael Daniel explained that the United States had to be "very judicious" about how it used sanctions as a tool of punishment because of their potential blowback in the form of the targeted states setting up an alternative financial system and "completely bypass[ing] New York."[155]

Unintended consequences were similarly a concern when policymakers debated the response to the 2014 Sony hack. On the one hand, the sense of asymmetric vulnerability meant that officials were worried about a North Korean counter-retaliation: "[a] cyber battle would be a lot more costly for the United States and its allies than for North Korea," cautioned Robert P. Silvers, the Assistant Secretary for Cyber Policy at the Department of Homeland Security at the time.[156] On the other, there was the issue of escalation. According to Clapper, officials debated a response to North Korea using cyber means, but they knew that the only way the United States could reach isolated North Korean infrastructure was by going through Chinese networks. Such action raised the prospect of escalation with China, as the operation could be considered an infringement on Chinese sovereignty. "The lawyers went nuts," according to Clapper, "so we didn't do anything on the cyber front. We ended up sanctioning a bunch of North Korean generals."[157]

---

[153] Ulrich Beck, 'The Terrorist Threat: World Risk Society Revisited', *Theory, Culture & Society* 19, no. 4 (1 August 2002): 42, https://doi.org/10.1177/0263276402019004003.
[154] Author interview with anonymous US Official, 20 August 2020.
[155] Author interview with Michael Daniel.
[156] Silvers quoted in: David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, 'The World Once Laughed at North Korean Cyberpower. No More.', *The New York Times*, 15 October 2017, sec. World, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.
[157] Clapper quoted in Waterman, 'Clapper'. This account is backed up by an interview provided to David Sanger by a participant in the National Security Council meetings: "… no one wanted to have the Chinese thinking that we were attacking them or using their networks to attack someone else." See: Sanger, *The Perfect Weapon*, 143.

Concerns about unintended effects were also present when the Obama White House was in the process of deciding how to respond to Russian election interference in 2016. First, however, it should be noted that when the true extent of the Russian influence operation was first discovered in early September 2016,[158] there were a number of political sensitivities which contributed to President Obama's decision not to publicly reveal the Russian campaign. Having already endorsed the Democratic Party nominee, Obama didn't want to be seen as influencing the vote, especially seeing as Hilary Clinton was leading in the pre-election polls.[159] Obama also didn't want to provide more publicity to the Russian campaign, which could have the effect creating distrust in the election and later undermining the authority of Clinton's presidency.[160] At the same time, while these concerns explain the lack of a public response, they do little to explain why the US didn't issue a covert response (we know it didn't thanks to a detailed and influential investigative report by *The Washington Post*, which revealed that covert measures were strongly considered but ultimately not implemented[161]).

Evidence indicates that a major reason why the Obama administration did not punish Russian activity were the perceived risks of unintended effects of a response, which outweighed the argument to issue a meaningful reprisal. Indeed, when asked about the response, Daniel explained that "the escalation risks were first and foremost in terms of how we thought about this."[162] *The Washington Post* report similarly affirmed that decision-makers did not implement more forceful responses due to a recurring concern that "any pre-election response could provoke an escalation from Putin," potentially in the form of a cyber operation targeting voting systems.[163] The perception of the risk of escalation as an obstacle to issuing a reprisal is corroborated by three further accounts.[164] One decision-maker explained that, "[i]f we got into a tit-for-tat on cyber with the Russians, it would not be to our advantage. … They could do more damage to us in a cyber war or have a greater impact."[165] Clapper was concerned about a potential Russian counter-response targeting American critical infrastructure, particularly electrical grids.[166] Ben Rhodes, Obama's Deputy National Security Advisor, wrote that Obama himself

[158] Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence*, 632.
[159] Ben Rhodes, *The World As It Is: Inside the Obama White House* (London: Penguin Random House, 2018), 399, 409.
[160] Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence*, 633.
[161] The article revealed that American officials had considered strong punishments in line with the warnings that had been issued to Russia in September and October 2016. After learning about the Russian intelligence service's campaign to disrupt the elections, Obama approved a covert measure authorising the planting of "cyber weapons" in Russian infrastructure. The administration had also contemplated the release of compromising material and sanctions that could "crater" the Russian economy. Yet, none of these were implemented. See: Miller, Nakashima, and Entous, 'Obama's Secret Struggle to Punish Russia for Putin's Election Assault'.
[162] Author interview with Michael Daniel.
[163] Miller, Nakashima, and Entous, 'Obama's Secret Struggle to Punish Russia for Putin's Election Assault'.
[164] These accounts were first discussed by Bruce Schneier in a blog post: Bruce Schneier, 'Attributing the DNC Hacks to Russia', 9 January 2017, https://www.schneier.com/blog/archives/2017/01/attributing_the_1.html.
[165] Anonymous decision-maker cited in: Michael Isikoff and David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump* (New York: Hachette Book Group, Inc., 2018), 194.
[166] Isikoff and Corn, 194.

feared Russia hacking into election day vote tabulations, which would amount to "hack[ing] the election itself."[167]

Many senior officials, including Susan Rice, Obama's National Security Advisor, knew that the eventual diplomatic and economic sanctions imposed by the outgoing president were not forceful enough to deter Russia in the future.[168] As Clapper revealed: "I didn't think the response was commensurate with what they'd done to us, but I also knew we weren't prepared to take more drastic steps."[169] The reason they were not prepared to take more drastic steps was the perception of the risks of inadvertent escalation that a meaningful punishment would entail.

In the case of the election interference, it is also important to consider an alternative explanation – the influence of individual cognitive and psychological factors. It is likely that the level of presidential involvement in the decision-making process would have been particularly high here given the salience of the case. The response itself also seems to align with what became known as "The Obama Doctrine": a set of principles which included caution, restraint in the use of force, and, incidentally, a concern about "the potential for unintended consequences."[170] How can we therefore determine if the decision was a product of Obama's individual biases or the risk society?

In this case, there is in fact evidence indicating that although Obama was closely involved with the decision-making, he did not reach the decision alone and nor did he dominate the decision-making process. First, the above quotes from senior officials and close advisors show that they held their own concerns about escalation – and likely passed on these views on to the president. Second, Ben Rhodes revealed that the decision-making process was a collective one, involving meetings comprised largely of "intelligence and cyber experts."[171] As Chapter 2 noted, on security issues involving technology, leaders are especially likely to rely on experts for guidance. This is particularly the case with cyber issues due to the virtual nature of the domain and its complexity. Given that there are strong indications that the decision on the response was taken in a group, it is possible to conclude that societal risk sensitivities likely played a more important role than individual beliefs, although the latter would have almost certainly reinforced the conviction to respond with restraint.

Officials working under the Trump administration also worried about inadvertent conflict escalation, although these concerns were less prominent than during the Obama administration

---

[167] Rhodes cited in: Peter Baker, 'How Trump's Election Shook Obama: "What If We Were Wrong?"', *The New York Times*, accessed 20 April 2020, https://www.nytimes.com/2018/05/30/us/politics/obama-reaction-trump-election-benjamin-rhodes.html; Rhodes, *The World As It Is: Inside the Obama White House*, 409.
[168] Isikoff and Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*, 284.
[169] Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence*, 659.
[170] Scholars have shown that the doctrine was informed by a strong desire to not repeat the mistakes of the US intervention in Iraq; on this see: Dominic Tierney, 'The Obama Doctrine and the Lessons of Iraq' (Foreign Policy Research Institute (FPRI), May 2012), https://www.fpri.org/docs/media/201205.tierney.obama-doctrine-iraq.pdf. From a cognitive standpoint, learning from historical failures makes sense: humans' "negativity bias" has been shown to explain leaders' inclination to learn from such events more than from successes. See: Johnson and Tierney, 'Bad World', 138.
[171] Rhodes, *The World As It Is: Inside the Obama White House*, 398.

(possibly due to the introduction of a new strategy of "persistent engagement," which we will discuss in the next section).[172] According to Fiona Hill, President Trump's Deputy Assistant and Senior Director for Russia at the National Security Council, "[t]here's a huge risk if we say we're going to take action through cyber retaliation." "If you do tit-for-tat vengeance, you always risk getting in a cycle."[173] Underscoring the level of attention paid to escalation concerns, Nakasone revealed that Cyber Command's operations to protect the 2018 mid-term elections were planned using stringent "risk assessments of escalation and other equities" (we will return to the discussion of this particular operation).[174] Finally, preventing further escalation was listed as a stated objective of the 2018 National Cyber Strategy.[175] What we will see, however, is that under the Trump administration, concerns about escalation did not hinder the United States in engaging in its own *preventive* cyber operations. While individual responses were still marked by weakness, for example in the previously discussed case of NotPetya, concerns about the nature of the operational environment in fact paved the way for the introduction of a much more confident preventive strategy.

Having shown how, in accordance with the expectations of the risk framework, US policymakers paid particular attention to the operational characteristics of the cyber domain that breed uncertainty, and, having proven that policymakers were constrained in issuing meaningful responses by their concerns about the risk of misattribution and the risk of unintended effects, the next section will discuss how the United States chose instead to engage in risk management practices to address the uncertainty inherent in the cyber domain.

4.5 US risk management practices: evolution from caution to proactiveness

As the risk framework explained, in practice risk societies are highly likely to prioritise risk management (resilience building, consequence management, and preventive action) as their central approach to cyber conflict in lieu of implementing reactive strategies like deterrence by punishment. Risk management practices are not intended to influence the resolve of the attacker – instead they reflect

[172] In the case of the Trump administration's response to the 2016 election interference, political considerations undoubtedly played a role. However, the reason this chapter doesn't investigate the factors that led to this response is because the time between the occurrence of the operation and the inauguration of President Trump means that any response taken by that administration would have lacked swiftness – which, according to the definition provided in Chapter 1, is a key element of meaningful punishment.
[173] Hill quoted in: Ellen Nakashima, 'Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader', *The Washington Post*, accessed 24 February 2021, https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html.
[174] Paul Nakasone, 'Statement of Paul M. Nakasone Commander United States Cyber Command before the House Committee on Intelligence and Emerging Threats and Capabilities', congress.gov, 4 March 2020, https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.
[175] The White House, 'National Cyber Strategy of the United States of America', 2.

an awareness that hostile cyber operations are an inevitable side effect of technological progress and thus need to be managed like other risks (for example terrorism or environmental disasters).

This section will consider the three risk management practices in turn under the Obama administrations and the Trump administration. It will show that, while the United States engaged in all three practices, preventive action over time became the preferred means for addressing the uncertainties inherent in the cyber domain. Although under the Obama administration there was already an indication of the willingness to implement preventive measures under the label of "active defense," it was under the Trump administration that this practice was brought into its full fruition with the introduction of the strategies of "persistent engagement" and "defend forward" (PE and DF). The strong embracement of preventive practices was, as the risk framework outlined, an outgrowth of policymakers' sensitivity to the cyber domain's complex adaptiveness, or, as US policy documents articulated it, the nature of cyberspace as an environment of "constant contact" and "shifting terrain."[176]

4.5.1 Increasing resilience

According to the risk framework, risk societies, recognising the inevitability of hostile cyber operations in the current stage of advanced modernity, will seek to increase the resilience of their digital infrastructures with the aim of mitigating some of their effects. Under the Obama administration, bolstering resiliency as a practice was most visible in the administration's efforts to improve general "cyber hygiene" across government and increase information sharing between the private and public sector. A 2013 executive order bound US government entities to disclose detected breaches to private sector companies.[177] Then, the Cybersecurity Information Sharing Act was signed into law in late 2015, encouraging companies to share information and authorising them to implement defensive measures on their systems to counter cyber threats.[178] Another resiliency initiative was the Cybersecurity Sprint, introduced by the White House in June 2015. The objective was to improve computer hygiene across the US government in thirty days, by introducing ubiquitous multifactor authentication, limiting the number of users with administrative privileges, and installing software patches.[179] As General Keith Alexander, then Commander of CYBERCOM, explained, "these capabilities [of state actors] are

[176] Goldman, 'From Reaction to Action'; U.S. Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 4.
[177] The White House, 'Executive Order -- Improving Critical Infrastructure Cybersecurity', 12 February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[178] Brad S. Karp, 'Federal Guidance on the Cybersecurity Information Sharing Act of 2015', Harvard Law School Forum on Corporate Governance, 3 March 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.
[179] Brendan I. Koerner, 'Inside the OPM Hack, the Cyberattack That Shocked the US Government', *Wired*, 23 October 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

expanding and there are real risks, which can only be managed by first fixing your own network security."[180]

The resiliency efforts initiated by the Obama administration were taken further by the Trump administration with the creation of the Cybersecurity and Infrastructure Security Agency, which was given a specific mandate to increase the resilience of US critical infrastructure.[181] Increasing resiliency for the purposes of "reducing the size of the attack surface at home" also appeared as a stated goal in the 2018 Command Vision for US Cyber Command.[182] Delivering on its promise, Cyber Command issued a series of disclosures of malware tools on Virus Total, an online repository. In a notable disclosure, CYBERCOM specified that the malware samples it uploaded had been attributed to North Korea and had previously aided the regime in pursuing illegal activities, including the stealing of funds for sanctions evasion.[183] The purpose of publicly disclosing the tools was to enable the private sector to build better defences and become more resilient, thus decreasing the impact of future cyber attacks and helping safeguard the health of the American economy.[184]

Finally, the 2017 National Security Strategy spelled out that "[r]educing risk and building more resilient communities are the best way to protect people, property, and taxpayer dollars from loss and disruption." Since "[s]ecurity was not a major consideration when the Internet was designed and launched," the government, in coordination with the private sector, "must design systems that incorporate prevention, protection, and resiliency from the start."[185]

4.5.2 Consequence management

According to the risk framework, risk societies, due to the same recognition of the inevitability of cyber attacks, will also tend to focus on managing their harmful consequences rather than engaging in risky reprisals for deterrence purposes. Both US administrations engaged in consequence management. The chapter already discussed the reasoning that determined the Obama administration's

---

[180] Alexander cited in: Joye, 'Interview Transcript'.
[181] Department of Homeland Security, 'About CISA', Official Website of the Department of Homeland Security, accessed 7 April 2020, https://www.cisa.gov/about-cisa.
[182] U.S. Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 6.
[183] USCYBERCOM Malware Alert, 'Malware Attributed to #NorthKorea by @FBI_NCIJTF Just Released Here: Https://T.Co/CBqSL7DJzI. This Malware Is Currently Used for Phishing & Remote Access by #DPRK Cyber Actors to Conduct Illegal Activity, Steal Funds & Evade Sanctions. #HappyValentines @CISAgov @DHS @US_CYBERCOM', *Twitter* (blog), 14 February 2020, https://twitter.com/cnmf_virusalert/status/1228309162284781569.
[184] Moreover, campaigns to "burn" adversary capabilities by disclosing them publicly have an additional benefit: by thwarting North Korea's sanctions evasion techniques, which rely significantly on hacking, they are an additional tool in managing the future risk of a nuclear rogue state. See: Shannon Vavra, 'Pentagon, FBI, DHS to Jointly Expose a North Korean Hacking Effort', CyberScoop, 14 February 2020, https://www.cyberscoop.com/hidden-cobra-malware-north-korea-fbi-dhs-dod-virus-total/.
[185] The White House, 'National Security Strategy of the United States of America' (The White House, December 2017), 13–14, https://nsarchive2.gwu.edu//dc.html?doc=4421220-The-White-House-National-Security-Strategy-of.

decision to not impose meaningful costs on Iran for the 2013 DDoS attacks on the financial sector. In this case, in line with the expectations of the risk framework, instead of issuing meaningful punishment, which would run the risk of triggering unintended effects, the administration decided to focus on managing the attack's consequences. US State Department and Homeland Security officials solicited the help of 120 countries to disrupt botnets – networks of Internet connected devices – on their territories that, unbeknown to the governments of these countries, were routing the attacks. Allies' computer emergency response teams (CERTs) were instructed to employ blackhole filtering, a process by which undesirable network traffic is forwarded and dropped at the edge of a network, to prevent the traffic from reaching US digital infrastructures.[186] They were also asked to patch vulnerabilities in their systems to effectively lock the adversary out. Importantly, showcasing the extent of policymakers' concern about potential escalation, the whole operation was conducted without encroaching on Iranian networks.[187]

Consequence management was also employed under the Trump administration. In the midst of and immediately after the NotPetya operation, The National Protection and Programs Directorate (NPPD), which is part of the US Department of Homeland Security, shared mitigation guidance to assist network defenders within private sector organisations in preventing further damage from the NotPetya malware. The NPPD also led the US government's incident response efforts and provided technical assistance to government organisations and private sector entities that had been infected by the malware.[188]

While the Trump administration continued the Obama administration's resiliency and consequence management efforts, the risk management practice that significantly dominated cybersecurity discussions among the policy community during this time was preventive action, to which we now turn.

4.5.3 Preventive action

Preventive action, as Chapter 3 explained, is the go-to practice of risk societies. In the United States, the tendency to favour preventive action for the purposes of managing risk can be seen as part

[186] Ellen Nakashima, 'Suspected Iranian Cyberattack on American Banks Led U.S. to Rally Support of 120 International Allies', *Washington Post*, 11 April 2014, sec. National Security, https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html; Cisco Systems, 'Remotely Triggered Black Hole Filtering— Destination Based and Source Based', Cisco, 2005, https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf.
[187] Nakashima, 'Suspected Iranian Cyberattack on American Banks Led U.S. to Rally Support of 120 International Allies'.
[188] US Department of Homeland Security, 'Written Testimony of NPPD for a Senate Committee on Armed Services Hearing Titled "Roles and Responsibilities for Defending the Nation from Cyber Attack"', Department of Homeland Security, 19 October 2017, https://www.dhs.gov/news/2017/10/19/written-testimony-nppd-senate-committee-armed-services-hearing-titled-roles-and.

of the precautionary principle line of thinking we discussed earlier, where, under conditions of uncertainty, it is believed that actions should be undertaken to prevent potentially adverse consequences or worst-case scenarios. The popularity of such thinking betrays a societal unwillingness to tolerate any potential harm or risk and a desire to try and impose some control over an external security environment, which is recognised as highly unpredictable.[189] The irony, as Chapter 3 stated, is that risk management can in itself produce new risks – although, as we will see below, the concern about preventive action potentially sparking escalation is likely exaggerated.

Preventive action, albeit under the term of "pre-emption," was encouraged as early as 2010 by Mike McConnell who had been the director of the NSA under Clinton. McConnell stated that pre-emption in cyberspace should be akin to US efforts in counterterrorism and involve "degrading, interdicting and eliminating … [adversaries'] leadership and capabilities to mount cyber attacks."[190] Eventually, flavours of this approach could be found in the strategy of active defence. Active defence as a concept goes back as far as 1996 and, although its definition has been through multiple iterations, it is generally understood to mean the US DoD engaging in defensive activities outside its own networks.[191] The crucial element of active defence refers to the proactive anticipation and disruption of attacks before these reach US territory.[192] This meant using "sensors, software, and intelligence to detect and stop malicious activity before it [could] affect DoD networks and systems."[193] In the event that malware did pass through undetected, it also included hunting for the adversary within the DoD's own networks.[194] While elements of the Obama administration's active defence might seem like a pre-cursor to the later strategies of persistent engagement and defend forward, active defence differed in practice from these strategies in its greater focus on securing internal networks "with a presumption against action."[195]

---

[189] Colin S. Gray, *National Security Dilemmas: Challenges and Opportunities*, 1st ed., Book Collections on Project MUSE (Washington, D.C.: Potomac Books, 2009), 226, https://muse.jhu.edu/book/41059/.
[190] Mike McConnell, 'Mike McConnell on How to Win the Cyber-War We're Losing', *The Washington Post*, 28 February 2010, https://cyberdialogue.ca/wp-content/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf.
[191] Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', 1.
[192] William Lynn III J., 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* 89, no. 5 (October 2010): 103; Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38, no. 2 (2013): 32–33, https://doi.org/10.1162/ISEC_a_00138.
[193] US Department of Defense, 'Department of Defense Strategy for Operating in Cyberspace', July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[194] Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy', 103.
[195] Author interview with anonymous US Official, 31 August 2020. Additionally, James Miller also explained in his interview that, "[t]here was one heavily-debated case where the US could have blunted an adversary's cyber attack and chose not to do so. It was known that this adversary was using only a fraction of its capabilities, and there was a concern that if you stop them from this limited attack, they are going to come back with something harder that you can't block… ." This incident also shows how fears of escalation meant that the Obama administration also was unwilling to engage in preventive action. See: Author interview with James Miller.

The introduction of PE and DF in 2018, spearheaded by Cyber Command, marked a significant shift in US cyber risk management.[196] As we already discussed, the new strategies were grounded in an understanding of cyberspace as an environment of "constant contact" and "shifting terrain," thus representing an evolution in policymakers' understanding and perception of the technical features of the domain and the adaptation of strategy to it.[197]

The Cyber Command Vision document explained that, by continually burrowing deep into US networks, adversaries were forcing the United States into a "reactive mode," which "introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success."[198] There was a clear preventive focus in the new strategy: "[w]e should not wait until an adversary is in our networks or on our systems to act with unified responses across agencies regardless of sector or geography," explained the document.[199] CYBERCOM thus shifted from being a "response force" to a "persistence force."[200]

As Chapter 3 already mentioned, prevention as a risk management strategy was first implemented in the United States as part of President Bush's 2002 National Security Strategy and was widely criticised on the grounds of embroiling the United States in protracted wars in the Middle East. The spillover from Bush's preventive action was the very embodiment of the notion that "risk management creates further risks," which Beck and the risk sociologists warned about. Although the geopolitical and operational context within which persistent engagement was introduced was very different, there are notable overlaps in some of the guiding assumptions of the Bush administration's strategy of anticipatory action and Cyber Command's preventive strategy under the Trump administration, which is why the strategy is worth discussing here. In both cases there was a marked emphasis on urgency of action and the necessity of disrupting potential threats before they materialised. For example, the 2002 Strategy stressed the need to abandon a reactive posture due to the "immediacy

[196] On a practical level, persistent engagement and defend forward were made possible after the Trump administration's elevation of Cyber Command to unified combatant command in May 2018 and the elimination of Presidential Policy Directive 20 (PPD-20), which had governed an elaborate interagency approvals process for offensive cyber attacks. As a result, the commander of Cyber Command gained more authority to take action. See: Dustin Volz, 'Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive', *Wall Street Journal*, 16 August 2018, sec. Politics, https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721.; US Naval War College, *2019 Future Warfighting Symposium: Emily Goldman, Cyber Strategy and Policy* (Newport, RI, 2019), https://www.youtube.com/watch?v=FxlvopfZ5Uc; Richard J. Harknett, 'United States Cyber Command's New Vision: What It Entails and Why It Matters', Lawfare, 23 March 2018, https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters; Richard J. Harknett, 'Progress Is the Promise in National Cybersecurity Strategy', Lawfare, 23 March 2020, https://www.lawfareblog.com/progress-promise-national-cybersecurity-strategy.

[197] U.S. Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 4.

[198] U.S. Cyber Command, 5.

[199] U.S. Cyber Command, 4–5.

[200] Paul M. Nakasone, 'A Cyber Force for Persistent Operations', *Joint Force Quarterly*, no. 92 (January 2019): 11.

of today's threats."[201] The overall focus of the 2002 Strategy was prevention (which, scholars argued, had mistakenly been called pre-emption[202]) and, as we discussed, "anticipatory action."[203] Similarly, the 2018 Cyber Strategy stressed the need to "pre-empt" hostile cyber actions and "defend forward by leveraging our focus outward to stop threats before they reach their targets."[204] Like Nakasone, the Cyber Command Vision cautioned that a "reactive posture introduces unacceptable risk."[205] In analysing US responses to cyber attacks and the evolution of the country's cyber policy, we therefore observe an adaptation of risk management strategies used for counterterrorism during the Bush era to the new environment of cyberspace. In interviews, policymakers who helped develop and implement PE and DF also noted parallels with previous counterterrorism logics.[206]

Referring back to the point of the risk sociologists that risk management produces new risks of its own, one major concern of some scholars about the new US approach was the idea that a more forward-leaning posture might produce unintended conflict escalation.[207] This is because PE and DF could be seen as introducing greater levels of uncertainty and friction for the adversary, which is known to intensify conflicts; competitive and continuous activity in adversary networks may also be subject to misinterpretation as offensive action, given the limitations of effective signalling in cyberspace.[208] These concerns seem particularly ironic given that, as we have discussed, the new preventive strategies were actually an outgrowth of the US risk society's overarching objective of managing future risks and uncertainty in the cyber domain and, within this, *escalation*. Indeed, as Thomas Wingfield, Deputy Assistant Secretary of Defense for Cyber Policy under the Trump administration, explained, "[w]e believe that inaction in cyberspace contributes to escalation more than reasonable action in cyberspace."[209] General Nakasone and Michael Sulmeyer wrote that reducing the risk of escalation was a "critical part of the planning process" for the new strategies and, like Wingfield, pointed out that "inaction poses its own risks" in terms of allowing damaging cyber campaigns to continue to penetrate US systems.[210]

---

[201] The White House, 'The National Security Strategy of the United States of America'.
[202] For a discussion of why Bush's strategy was preventive rather than pre-emptive see: Michael W. Doyle, 'Striking First', in *Striking First: Preemption and Prevention in International Conflict*, ed. Stephen Macedo, University Center for Human Values Series (Princeton, NJ: Princeton University Press, 2008), 25, https://ezproxy-prd.bodleian.ox.ac.uk/login?url=https://www.jstor.org/stable/10.2307/j.ctt7t7md.
[203] The White House, 'The National Security Strategy of the United States of America', 16.
[204] Department of Defense, 'Summary: Department of Defense Cyber Strategy', 2.
[205] U.S. Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 5.
[206] Author interview with Emily Goldman; Author interview with Gary Corn.
[207] Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace'.
[208] Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *The Cyber Defense Review*, 2019, 270, https://doi.org/10.2307/26846132.
[209] Wingfield quoted in: Eric Tucker, 'US, Estonia Partnered to Search out Cyber Threat from Russia', AP NEWS, 3 December 2020, https://apnews.com/article/hacking-russia-estonia-e931e674091b080f7a01642b01729bbe.
[210] Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace', *Foreign Affairs*, 25 August 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Alongside the reassurances of policymakers, there are also other reasons to believe that the scholarly concerns about escalation from PE and DF might be overblown. If this is true, then Beck's notion that risk management begets further risk in a never-ending loop might actually be less pronounced in the cyber domain. PE and DF campaigns were designed to be limited and measured, precisely to prevent triggering a reprisal from adversaries that could escalate into a wider conflict.[211] Moreover, most actions under persistent engagement are understood to be covert in nature. Indeed, Lennart Maschmeyer argued that in order to be successful, they must be both covert and clandestine, as otherwise they risk being prematurely neutralised.[212] Hiding such operations from outside audiences, while potentially problematic for reasons of public accountability, can in itself be an indication of restraint and wanting to manage the risk of escalation by keeping the rivalry "under the radar."[213] The empirical record of operations under PE and DF also shows no indication of sparking escalation. In an operation known as the "IRA takedown," American operatives temporarily disabled the servers of the Russian Internet Research Agency before the 2018 mid-term elections in an effort to prevent the kind of interference that the Agency had orchestrated during the 2016 presidential vote.[214] What this operation showed was that it was possible for the United States to engage in preventive action and not provoke a public reaction or retaliation from the adversary, in this case Russia. The IRA takedown, in other words, certainly did not result in escalation.[215]

The key difference thus between the proactive risk management strategies employed during the Bush era and under the Trump administration was the definitive move away from violence and overt aggression towards non-violence, covertness, and continuous engagement in preventive practices. Whereas under Bush, prevention meant armed intervention, in the context of the cyber domain under the Trump administration, it meant encroaching on enemy territory, so-called "red space," to disrupt

---

[211] Julian E. Barnes, 'U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections', *The New York Times*, 23 October 2018, sec. U.S., https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

[212] Lennart Maschmeyer, 'Persistent Engagement Neglects Secrecy at Its Peril', Lawfare, 4 March 2020, https://www.lawfareblog.com/persistent-engagement-neglects-secrecy-its-peril.

[213] Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, New Jersey: Princeton University Press, 2018), 296. The desire for escalation avoidance is also evident in recent academic scholarship, particularly in the work of Richard Harknett, Emily Goldman, and Michael Fischerkeller, all of whom have been influential in informing the new strategies Goldman, 'From Reaction to Action'; Fischerkeller and Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation'. Addressing the issue of escalation specifically, Fischerkeller and Harknett have sought to show that persistent engagement will "inhibi[t] adversary efforts to increase the scale, scope, and/or intensity of cyber operations/ campaigns" and therefore maintain competitive interaction dynamics below the threshold of armed conflict and within the bounds of agreed competition. See: Fischerkeller and Harknett, 276.

[214] Ellen Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms', Washington Post, 27 February 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[215] One US senator, having listened to a classified briefing on the IRA operation, lamented the fact that the American public would not be able to learn more about its achievements. See: Ellen Nakashima, 'U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms', Washington Post, 15 February 2019, https://www.washingtonpost.com/world/national-security/us-cyber-force-credited-with-helping-stop-russia-from-undermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a-0ab2f17e305b_story.html.

adversary operations and capabilities covertly and without the use of force. In communicating more openly about the policies of PE and DF, the United States sought to signal to adversaries its non-escalatory intent and thereby limit misperceptions. By establishing a constant presence in adversary networks, it was possibly trying to gain a solid understanding of these systems in an effort to minimise the unintended effects of subsequent operations there, such as the spread of malware (and thus manage the risk of escalation). By gaining an insight into adversary toolkits, US cyber operators were able identify and patch vulnerabilities in US systems, thus decreasing the attack surface at home and mitigating the risks of future attacks that might require a response. Thus, in their mission to manage escalation risks, preventive practices in the form of PE and DF seem to make them a particularly appropriate choice for risk-intolerant societies.

4.6 Conclusion

This chapter sought to demonstrate that US policymakers were unwilling to accept the risks created by the technical characteristics of the cyber operational environment and issue meaningful punishments. The overwhelming attention that policymakers paid to how these characteristics increased US vulnerability and complicated the response calculus are the result of a central underlying societal concern: avoiding and minimising risk.

The chapter started with an overview of the most significant cyber incidents that the United States fell victim to since 2010 and showed how these had a significant impact on national security. It then moved on to explaining the historical and cultural sources of the US risk society. The remainder of the chapter sought to demonstrate that the risk society paradigm operating within policy circles was the source of weak responses. The main argument of the chapter was that cultural risk sensitivity influenced the decision-making processes of US policymakers in such a way as to make them unwilling to accept the risks of issuing a meaningful punishment. As the analysis of the cases of the Iranian DDoS attacks, the Sony Pictures hack, and the 2016 election interference demonstrated, policymakers perceived the risks of inadvertent escalation to be particularly prominent, which is consistent with the risk framework's expectations. Indeed, the chapter showed that policymakers were particularly sensitive to the cyber domain's complexity and the proliferation of capabilities as these gave them a sense of the domain's uncontrollability and the potential for unintended effects, including inadvertent escalation. Anxiety about the loss of control and the unpredictability of future scenarios are, as Chapter 2 showed, the quintessence of the risk society. In their unease about the uncertainties inherent in the operational domain, US policymakers were also hindered by the need for near certainty in the attribution of attacks; the chapter showed that, in this way, the risk of misattribution and plausible deniability posed an obstacle for swift, and therefore meaningful, punishment.

In the case of the 2016 election interference, the chapter noted that individual biases, particularly President Obama's cautious disposition, could have also played a role in producing a

restrained response. However, while Obama's time at the White House was indeed marked by careful deliberation and caution,[216] it is notable that the decision in this case was made in consultation with a larger group of experts. Moreover, responses to cyber attacks by the Trump administration were similarly weak, which indicates that there were factors other than Obama's individual disposition that were common to both administrations in informing their unwillingness to punish meaningfully.

The case study analysis also showed that, consistent with the expectations of Chapter 3, the United States engaged in practices of risk management, including increasing resilience, consequence management, and preventive action. It noted that the application of preventive risk management practices was particularly embraced under the Trump administration. The adoption of a bolder approach to risk management under Trump was shown to have been due to the evolution of ideas over time on how to best avoid risk in the cyber domain, informed particularly by the understanding of the cyber domain as an environment of "constant contact," which grew out of a concern about the complexity and interconnectedness of the operational environment.

In sum, the analysis presented in this case study sought to show that the risk framework provides a convincing explanation as to why the United States didn't respond to damaging cyber attacks with meaningful punishment. The analysis of interview data, policymakers' statements, and government documents indicated that the risk paradigm was the dominant mode of thinking which set the tone for US responses to cyber attacks and guided the United States' general approach to cyber conflict in the form of risk management practices. This was the case under both the Obama administrations and the Trump administration.

[216] Philip Stephens, 'Cautious President Deserves Second Term', *Financial Times*, 1 November 2012, https://www.ft.com/content/0c44ade8-22c2-11e2-938d-00144feabdc0.

Chapter 5
Israel and the Culture of Over-Punishment: The Threat Society in Action

Israel wants to deter cyber attacks. Israel wants to deter almost everything it sees. It's in our blood. We will not allow any kind of attack.

Senior Military Cyber Defence Official (Israeli Defence Forces)[1]

5.1 Introduction

Israeli responses to cyber operations meet the criteria for meaningful punishment: they were swift, severe, and transparent.[2] This chapter will argue that a set of features from strategic culture, prevalent across Israeli society, created Israel's threat society identity and profoundly shaped Israelis' perception and interpretation of material dangers and thus lay at the root of Israel's choice to issue meaningful responses to cyber attacks. First, as a result of the *siege mentality*, Israel was mainly preoccupied with one particular, well-defined existential threat (as opposed to diverse and potential risks).[3] Consistent with Beck's critical realism, this chapter proposes that while external threats against Israel were grounded in a material reality, threat perception, like risk perception, was shaped by the country's history and culture, leading Israel to view the external threat as existential.[4] Second, the Israeli *problem-solving attitude*, manifested in a willingness to address security challenges "head on," translated into swift reactivity. Third, the *cult of the offense*, the strong preference for offensive military operations over defensive measures, encouraged risk-taking in strategic decision-making and forceful responses to adversary behaviour. The concept of the threat society thus helps us to understand the consequences of strategic culture for state behaviour – in other words, it is a guiding concept that elucidates the causal variable of the argument of this thesis.

Although Iran presented a real material threat, it need not have been perceived as existential. What emerged from the interviews for this case study was that it was, in fact, a set of ideas inherent in strategic culture that guided Israel in perceiving the Iranian threat as *existential* and created the country's threat society identity, which in turn produced its risk-accepting responses to cyber attacks.

---

[1] Author interview with senior military cyber defence official, 9 January 2021.
[2] A note on the sources used for this case study: many of the interviews used in this chapter are anonymised due to the sensitive nature of the interviewees' work. In addition, as a result of the same sensitivities, the majority of the anonymous interviewees were former senior military or intelligence officials, but some had left their senior leadership roles as recently as two weeks before the interviews took place.
[3] As Chapter 2 explained, threats are different to risks as they are typically well-defined and constructed against a specific state actor. See: Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006), 49.
[4] Ulrich Beck, *World Risk Society* (Cambridge: Polity, 1999), 135.

Strategic culture is a particularly potent force in Israeli society due to the existence of compulsory military service and the "revolving door" between the Israeli Defence Forces (IDF) and government.[5]

The chapter will seek to show that the logic guiding Israeli decision-making on responses to cyber attacks was the same logic that is used in the kinetic domain: the desire to postpone the next war with an adversary perceived to be ideologically committed to Israel's annihilation. Israeli policymakers applied the same strategic thinking in the cyber domain as they do in other domains – a strategy of conventional deterrence, which rests on building a reputation for costly retaliation.

Focusing particularly on policies and decisions made during the second Netanyahu administration (April 2009 to June 2021), this chapter addresses the research question of the thesis by arguing that Israel, as a threat society, was not dissuaded from punitive action by the operational characteristics of the environment and did not perceive the risks of escalation as an obstacle to meaningful responses. In fact, Israeli policymakers did not view the cyber domain as a distinct strategic environment requiring unique strategic frameworks – their focus was instead on retaliating for *any* acts of Iranian aggression in order to build Israel's reputation as a militarily superior, credible punisher and, in so doing, they believed, secure Israel's continued existence.

The chapter is organised as follows. First, it will describe the cyber attacks that affected Israel and detail Israel's responses. Second, it will discuss the features of Israeli strategic culture that created the threat society and are therefore most distinctive for understanding how Israel responded to foreign threats, including cyber attacks. Third, the chapter will demonstrate that the threat society identity shaped Israel's conventional deterrence strategy and the interpretation of the material threat of Iran as existential, which in turn meant that the country responded to cyber attacks meaningfully. This argument will be illustrated on the basis of Israel's response to the Iranian attack on Israel's water infrastructure in 2020. Finally, the chapter will consider the Israeli preventive strategy of "the campaign between wars" (CBW), showing that this strategy provides further evidence of Israel's risk-acceptant attitude, and will briefly analyse the country's engagement in resilience building and consequence management. It will argue that the preventive strategy of the CBW cannot accurately be described as a risk management practice due to its stated deterrence objective and show that, while Israel did engage in resilience-building and consequence management, these practices were not regarded as some of the primary tools for addressing cyber conflict.

[5] Michael I. Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', in *The Making of Strategy: Rulers, States, and War*, ed. Williamson Murray, Macgregor Knox, and Alvin Bernstein (Cambridge, UK: Cambridge University Press, 1994), 555.

5.2 An overview of cyber attacks targeting Israel and its responses

Israel possesses advanced cyber capabilities.[6] Among the first known demonstrations of its cyber prowess was in 2007 when the country reportedly disrupted Syria's air defence system using an "air-to-ground hack," the purpose of which was to aid the bombing of a suspected Syrian nuclear facility in Al-Kibar. As a result, the Syrian air defence system failed to identify the eight Israeli Air Force aircraft that conducted the strike.[7]

In terms of responses to cyber attacks, there are two particular incidents which illustrate Israel's willingness to punish meaningfully. The first of these took place in May 2019 during a weekend of fighting between Israel and Palestine in the Gaza Strip.[8] In the first ever instance of "immediate military retaliation" for a cyber attack, Israel launched an air strike on an empty building used by Hamas cyber operatives.[9] The only information available publicly about the cyber operation that Hamas had been conducting came from the commander of the IDF, Brigadier General "Dalet," identified only by the first Hebrew letter of his name, who explained that the operation had happened the day before the Israeli strike and was aimed at "harming the quality of life of Israeli citizens."[10] In a rare disclosure, the Israel Defense Forces publicly took responsibility for the reprisal, announcing in a taunting tweet: "[w]e thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed."[11] The use of the word "thwarted" here, according to one well-informed interviewee, was intended to convey that Israel minimised the damage of the operation (as opposed to stopping it before it reached Israeli networks).[12]

Another incident that showcased Israel's willingness to retaliate came after an attack on Israel's water supply and treatment facilities in April 2020. The attack, as it later became clear, was an Iranian malware operation, routed via servers in the United States and Europe to obscure its origins. It sought to manipulate the software controllers of water pumps so as to increase the amount of chlorine added to the water in two Israeli pumping stations, which provide fresh water and wastewater removal to

---

[6] Lior Tabansky, 'Israel Defense Forces and National Cyber Defense', *Connections* 19, no. 1 (2020): 47.
[7] Kim Zetter, 'Hacker Lexicon: What Are CNE and CNA?', *Wired*, 7 June 2016, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/; Tabansky, 'Israel Defense Forces and National Cyber Defense', 54.
[8] Judah Ari Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle', The Times of Israel, 5 May 2019, https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/.
[9] Zak Doffman, 'Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First', Forbes, 6 May 2019, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/; Jerusalem Post Staff, 'Hamas Cyber-Attack Thwarted by Israel Security Forces', The Jerusalem Post, 5 May 2019, https://www.jpost.com/breaking-news/hamas-cyber-attack-thwarted-by-israel-security-forces-588852.
[10] Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle'.
[11] Israel Defense Forces (IDF), 'CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets.', Twitter, 5 May 2019, https://twitter.com/IDF/status/1125066395010699264.
[12] Author interview with former senior executive at the Israel National Cyber Directorate, 16 December 2020.

districts with residential, medical, and commercial customers – but ultimately failed in this objective.[13] Nevertheless, the attack was regarded in Israel as particularly significant because the country considers water facilities to be part of its critical infrastructure.[14] Commenting on the attack, Yigal Unna, the Director General of the National Cyber Directorate, stated that, "[t]he attempted attack on Israel was coordinated and organized with the aim of harming our humanitarian water system, and had it succeeded, we would have been forced to deal with damage to the civilian population, and even with a temporary water shortage that could have caused extensive damage and disaster."[15] He continued, "[r]apid is not something that describes enough how fast and how crazy and hectic things are moving in cyberspace and I think we will remember this last month and May 2020 *as a changing point in the history of modern cyber warfare* [emphasis added]."[16]

Although the attack was never publicly attributed to Iran by Israel, Israel reportedly retaliated against Iran for the operation in May in the form of a sophisticated cyber attack on Shahid Rajaee Port, which processes almost half of Iran's foreign trade.[17] A foreign security official who monitored the evolution of the Israeli attack described its consequences as being "total disarray"; satellite imagery showed that the attack halted the port's shipping traffic for at least 4 days and resulted in large backups on waterways and roads leading to the port.[18] The choice of target was likely symbolic: the city of Bandar Abbas, where the port is located, houses the naval headquarters of the Islamic Revolutionary Guard Corps and the port often serves as the point of departure for Iranian shipments of weapons. Iran also uses the Revolutionary Guards fleet to interfere with shipping traffic in the Persian Gulf.[19] The port

[13] Mehul Srivastava, 'Israel-Iran Attacks: "Cyber Winter Is Coming"', Financial Times, 31 May 2020, https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967; Joby Warrick and Ellen Nakashima, 'Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran', *Washington Post*, 8 May 2020, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.

[14] Ronen Bergman and David M. Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks', *The New York Times*, 20 May 2020, sec. World, https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

[15] Unna cited in: David Siman-Tov and Shmuel Even, 'A New Level in the Cyber War between Israel and Iran', *INSS* (blog), 3 June 2020, http://www.inss.org.il/publication/iran-israel-cyber-war/.

[16] AP and TOI staff, '"Cyber Winter Is Coming," Warns Israel Cyber Chief after Attack on Water Systems', The Times of Israel, 28 May 2020, https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/.

[17] Bergman and Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks'; Srivastava, 'Israel-Iran Attacks'.

[18] JD Work and Richard Harknett, 'Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges', Issue Brief (Washington, D.C.: Atlantic Council Scowcroft Center for Strategy and Security, July 2020); Joby Warrick and Ellen Nakashima, 'Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility', *Washington Post*, 18 May 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[19] Omer Dostri, 'Cyber-Warfare between Iran and Israel', JISS, 3 June 2020, https://jiss.org.il/en/dostri-cyber-warfare-between-iran-and-israel/.

is the most important maritime gateway into the country, handling 85 per cent of Iran's shipping cargos.[20]

The decision to retaliate for the Iranian attack was reportedly taken by Naftali Bennett, then Israel's acting Defence Minister, who had insisted on a visible response – shortly after the retaliation he commented that "the Iranian octopus is sending his tentacles to grab onto us from all directions … We must increase political, economic, military, and technological pressure, and act in other dimensions as well."[21]

While Israel did not officially take responsibility for the retaliation, Israel's role in the attack was disclosed by a number of anonymous Israeli officials in interviews with credible media outlets.[22] In addition, Amos Yadlin, a former head of IDF military intelligence, went on the record stating that, "[t]he attack displayed the cyber ability of a world power. It appears that this was a clear Israeli message to Iran, don't dare to touch civilian systems, the water and electricity systems in Israel, which were attacked this past month. You, the Iranians, are more vulnerable than we are."[23] Iran also acknowledged that a foreign actor was responsible for taking the port's computers offline.[24]

The lack of a clear statement from Israel regarding its responsibility for the operation is not unusual: Israeli officials, particularly members of the IDF, often maintain ambiguity regarding the military's activities.[25] While scholars have linked states' decisions not to claim or deny their offensive operations to wanting to alleviate outside pressure on the opponent to hit back (in other words, allowing the opponent to "save face" and not escalate),[26] Gabi Siboni, Head of the Cyber Security Program at the Institute for National Security Studies (INSS) and senior consultant to the IDF, linked such a posture in Israel to his country's strategic culture: "[t]here is a strategic culture of not attributing your own activity in Israel. There is no tribunal you have to justify your activity in front of. You don't need to go to the UN and say: 'we are Israel and we allegedly attacked this port in Iran because this is the proof that Iran tried to do something to us.'"[27] The reason that the existing scholarly explanations for states'

---

[20] SeaNews, 'Iran Plans to Bring Its Shahid Rajaee Port to State-of-Art Status', SeaNews Turkey, 7 September 2019, https://www.seanews.com.tr/iran-plans-to-bring-its-shahid-rajaee-port-to-state-of-art-status/183880/.
[21] Siman-Tov and Even, 'A New Level in the Cyber War between Israel and Iran'; Srivastava, 'Israel-Iran Attacks'.
[22] Bergman and Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks'.
[23] Yadlin cited in: AP and TOI staff, '"Cyber Winter Is Coming," Warns Israel Cyber Chief after Attack on Water Systems'.
[24] Michael Bachner and TOI Staff, 'By Design, Cyberattack on Iran Port Caused Only Minor Damage – Report', The Times of Israel, 20 May 2020, https://www.timesofisrael.com/by-design-cyberattack-on-iran-port-caused-only-minor-damage-report/.
[25] Rory Cormac and Richard J. Aldrich, 'Grey Is the New Black: Covert Action and Implausible Deniability', *International Affairs* 94, no. 3 (1 May 2018): 489, https://doi.org/10.1093/ia/iiy067; Bachner and TOI Staff, 'By Design, Cyberattack on Iran Port Caused Only Minor Damage – Report'.
[26] Cormac and Aldrich, 'Grey Is the New Black'; Austin Carson, 'Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War', *International Organization* 70, no. 1 (ed 2016): 104–5, https://doi.org/10.1017/S0020818315000284; Austin Carson and Keren Yarhi-Milo, 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret', *Security Studies* 26, no. 1 (2 January 2017): 133, https://doi.org/10.1080/09636412.2017.1243921.
[27] Author interview with Gabi Siboni, 17 December 2020. Gabi Siboni is also a retired colonel of the IDF.

covert action are less helpful in elucidating Israel's motivations is because Israel is not particularly sensitive to the risks of escalation – as the later discussion in the chapter will reveal, Israel is in fact risk-acceptant in this regard and maintains a constant state of limited war with Iran under the campaign between wars, which even includes air strikes.[28] As we will also see later, while Israel generally does want to postpone the outbreak of a regional *armed conflict* in order to give itself time to rearm and create the best conditions for eventually defeating the adversary, it is guided by the logic that escalating first can be a useful means of demonstrating superiority of force over the adversary and, in the medium and long term, deterring it from further aggression.

Finally, Israel has also been on the receiving end of cyber operations perpetrated by non-state sponsored hacktivist groups. Most notably, between 2012 and 2014, the country was targeted several times by the group Anonymous in a series of website defacements, distributed denial of service (DDoS) attacks, and data leaks.[29] The operations were a response to Israel's military involvement in Gaza.[30] Since 2013, Anonymous has also been coordinating an annual "OpIsrael" attack, mainly involving DDoS attacks, on the 7th of April.[31] The Israeli government has consistently maintained that these attacks have been unsuccessful and caused minimal damage.[32] For example, in 2013 the websites targeted by Anonymous belonged mainly to small businesses, without any connection to the government, and the personal data leak was comprised of email addresses and passwords of ordinary people stolen from an Israeli real estate website.[33] A pro-Israel hacker group also launched a counter-operation, targeting Arabic websites and exposing individual hackers affiliated with Anonymous.[34] For a country experiencing thousands attacks of on its government websites per month, the Anonymous operations, while potentially embarrassing, were not noted as a significant national security incident.[35]

---

[28] Carson, 'Facing Off and Saving Face', 105.
[29] Olga Khazan, 'Anonymous Is Hacking Israeli Web Sites', *Washington Post*, 17 November 2012, https://www.washingtonpost.com/news/worldviews/wp/2012/11/17/anonymous-is-hacking-israeli-web-sites/; Haviv Rettig Gur, '"Anonymous" Escalates Cyber-War against Israel and pro-Israel Groups', The Times of Israel, 16 November 2012, http://www.timesofisrael.com/anonymous-escalates-cyber-war-against-israel-and-pro-israel-groups/; Adam Clark Estes, 'Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back', The Atlantic, 8 April 2013, https://www.theatlantic.com/international/archive/2013/04/anonymous-hits-israel-massive-cyber-attack-israel-attacks-back/316538/.
[30] Gur, '"Anonymous" Escalates Cyber-War against Israel and pro-Israel Groups'.
[31] Nitsan Saddan, 'Anonymous' "Hack Israel Day" Could Impact the Entire World', Vox, 7 April 2016, https://www.vox.com/2016/4/7/11585928/anonymous-hack-israel-day-could-impact-the-entire-world; TOI staff, 'Israeli Sites Hacked to Display: "Jerusalem Is the Capital of Palestine"', 4 April 2018, https://www.timesofisrael.com/israeli-sites-hacked-to-display-jerusalem-is-the-capital-of-palestine/.
[32] John D. Sutter, 'Anonymous Declares "cyberwar" on Israel', CNN, 20 November 2012, https://www.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html; Associated Press, 'Anonymous Hacker Attack on Israeli Websites "Causes Little Real Damage"', The Guardian, 8 April 2013, http://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites; Dennis Mitzner, 'Israel Prepares for #OpIsrael Cyberattack', *TechCrunch* (blog), 4 April 2016, https://social.techcrunch.com/2016/04/04/israel-prepares-for-opisrael-cyberattack/.
[33] Sam Biddle, 'Anonymous Is Losing Its War Against Israel', Gizmodo, 19 November 2012, https://gizmodo.com/anonymous-is-losing-its-war-against-israel-5961685.
[34] David Shamah, '"Anonymous" a Little Less so, Thanks to Israeli Hackers', Times of Israel, 24 May 2013, http://www.timesofisrael.com/anonymous-a-little-less-so-thanks-to-israeli-hackers/.
[35] Estes, 'Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back'.

Having provided an overview of the most notable cyber attacks targeting Israel, the following section will explore the roots of the country's resolve to respond meaningfully.

5.3 The sources of meaningful responses: strategic culture and the threat society

This section will focus mainly on the three elements of strategic culture that create the Israeli threat society in order to lay the conceptual ground for the later analysis of Israel's responses. Scholars sceptical of cultural explanations for national security decision-making might argue that, in Israel's case, the country's intense geopolitical rivalry with its regional competitors is the primary factor informing Israel's security posture and eclipses any cultural factors. To dispel this scepticism, the discussion here will start with exploring the realities of Israel's geopolitical situation, especially vis-à-vis Iran, and show that Iran's acquisition of nuclear weapons need not necessarily be interpreted as a threat to Israeli existence – in other words, the Israeli interpretation is not solely a product of objective material realities. The rest of the section will then turn to exploring the elements of Israeli strategic culture that shape Israeli perceptions of its own security situation and create the country's threat society identity.

Apart from a few countries such as Egypt and Jordan that have recognised Israeli statehood, Israel remains largely unrecognised by other countries in its region.[36] Over the last two decades, one of those countries, Iran, has become Israel's main and historically most sophisticated national security threat.[37] Although Iran began to support the creation of Hezbollah already in the 1980s, Israel only started to see Iran as a potential existential challenge once the country rapidly progressed with its missile and nuclear programs in the 1990s after the Iran-Iraq war.[38] The 2003 Iraq war served to cement Iran as Israel's number one adversary after Saddam Hussein had been removed as a common enemy.[39] The subsequent 2006 Lebanon war, although fought between Hezbollah and Israel, was widely seen as a proxy war with Iran and showcased the country's effectiveness in supporting military operations against Israel.[40] Lebanese Hezbollah was in fact the first direct proxy militant group of the Islamic Republic, tasked with spreading the Islamic Revolution in Lebanon and confronting Israel.[41] By arming Hezbollah, Hamas, and Palestinian Islamic Jihad in support of their operations against Israel and, more

---

[36] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 534.
[37] Dalia Dassa Kaye, Alireza Nader, and Parisa Roshan, *Israel and Iran: A Dangerous Rivalry* (Santa Monica, CA: RAND National Defense Research Institute, 2011), x, 1; Charles Freilich, 'Israel's National Security Policy', in *The Oxford Handbook of Israeli Politics and Society*, ed. Hazan Reuven et al. (Oxford: Oxford University Press, 2021), 418.
[38] Kaye, Nader, and Roshan, *Israel and Iran*, 21.
[39] Kaye, Nader, and Roshan, 21.
[40] Kaye, Nader, and Roshan, xi.
[41] Ilan Goldenberg et al., 'Countering Iran in the Gray Zone: What the United States Should Learn from Israel's Operations in Syria' (Center for a New American Security, 2020), 2, https://www.jstor.org/stable/resrep24223.7; Kevin Whitelaw, 'Ahmadinejad: Holocaust "Opinion Of Just A Few"', NPR.org, 25 September 2009, https://www.npr.org/templates/story/story.php?storyId=113171156.

recently, by establishing military and strategic dominance in Syria, Iran has been able to extend its military reach into Israel.[42]

Israel's main concerns, however, refer to the development of Iran's suspected nuclear programme. First and foremost, Israel believes that nuclear capabilities would embolden Iran and lead it to attempt to expand its zone of influence to the Gulf region and Levant area.[43] Second, an Iranian nuclear capability might also result in increased aggression from the regime's allies, including Syria and Hezbollah.[44] Moreover, Israelis fear that such a development might weaken the regional influence of Israel's US ally and could lead to regional realignment among Arab states.[45] Finally, Israel believes that Iran "going nuclear" could result in regional nuclear proliferation, mainly in Saudi Arabia, Egypt, and Turkey.[46]

At the same time, given Israel's overwhelming nuclear superiority over Iran,[47] it is important to consider that a nuclear-armed Iran would only pose an existential threat to Israel if the regime were willing to endure damage at home so severe that it would be akin to "national suicide."[48] Kenneth Waltz wrote in 2012 that while the leaders of the Iran indulge in inflammatory rhetoric, "they show no propensity for self-destruction."[49] Indeed, in stark contrast to Iran's ideological anti-Semitic proclamations stands its largely rational pattern of behaviour involving nuclear issues.[50] According to Waltz, the existential threat of a nuclear Iran has in fact been greatly exaggerated by Israel; Iran's acquisition of nuclear weapons could actually stabilise the Middle East by reducing imbalances in military capability between the regional powers.[51] Moreover, wrote Waltz, the historical record, particularly the cases of China, India, and Pakistan, shows that states tend to become more cautious after acquiring nuclear capabilities as they are aware that this makes them a potential target of major

---

[42] Farzin Nadimi, 'Iran and Israel's Undeclared War at Sea (Part 2): The Potential for Military Escalation', The Washington Institute, 13 April 2021, https://www.washingtoninstitute.org/policy-analysis/iran-and-israels-undeclared-war-sea-part-2-potential-military-escalation; Oula A. Alrifai, Nakissa Jahanbani, and Mehdi Khalaji, 'Iran's Long Game in Syria', The Washington Institute, 25 March 2021, https://www.washingtoninstitute.org/policy-analysis/irans-long-game-syria; Lazar Berman, 'Iran Showing Increasing Nerve as Fight with Israel Spreads to the Sea', The Times of Israel, 26 March 2021, https://www.timesofisrael.com/iran-showing-increasing-nerve-as-fight-with-israel-spreads-to-the-sea/; Isabel Kershner, 'Iran Fires Rockets Into Golan Heights From Syria, Israelis Say', *The New York Times*, 9 May 2018, sec. World, https://www.nytimes.com/2018/05/09/world/middleeast/israel-iran-attack.html.

[43] Kaye, Nader, and Roshan, *Israel and Iran*, 1, 5, 27; Ehud Eiran and Martin B. Malin, 'The Sum of All Fears: Israel's Perception of a Nuclear-Armed Iran', *The Washington Quarterly* 36, no. 3 (1 August 2013): 80, https://doi.org/10.1080/0163660X.2013.825551.

[44] Eiran and Malin, 'The Sum of All Fears', 80.

[45] Kaye, Nader, and Roshan, *Israel and Iran*, 29.

[46] Eiran and Malin, 'The Sum of All Fears', 80–81; Freilich, 'Israel's National Security Policy', 418.

[47] Israel has never officially confirmed its nuclear capability, but, according to the Nuclear Threat Initiative, it is widely understood that the country possesses a "sizeable nuclear arsenal." See: NTI, 'Israel Country Page', NTI, July 2017, https://www.nti.org/learn/countries/israel/.

[48] Gil Merom, 'Israeli Perceptions of the Iranian Nuclear Threat', *Political Science Quarterly* 132, no. 1 (2017): 106, https://doi.org/10.1002/polq.12574.

[49] Kenneth N. Waltz, 'Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability', *Foreign Affairs* 91, no. 4 (2012): 4.

[50] Merom, 'Israeli Perceptions of the Iranian Nuclear Threat', 103.

[51] Waltz, 'Why Iran Should Get the Bomb', 3.

powers.[52] Finally, Waltz pointed out, Iran acquiring the bomb is not likely to lead to regional nuclear proliferation, evidenced by the more general slowdown in the emergence of nuclear-capable states since 1970.[53]

If Waltz is correct, then there must be other factors than just the emergence of Iran as a potential national security challenger fuelling the Israeli societal fixation on the existential threat posed by the country. After all, given Israel's conventional and nuclear superiority over Iran and its other neighbours, Israel is no longer the besieged state fighting for survival as it was seven decades ago; rather, despite its small size (just 9,600 square miles) and narrow geography, Israel has become an established (if officially unconfirmed) nuclear power; its continued existence seems secure, even in a hostile and volatile region.[54] What is more, a shared animosity towards Iran has led to indirect diplomatic coordination with some of Israel's formerly hostile neighbours – Saudi Arabia and other Gulf states – thus potentially contributing to Israel's security within the region.[55]

As several interview subjects revealed, the sense of existential threat that permeates Israeli society is more a feature of the country's strategic culture than a result of external security conditions. According to Ken Booth, strategic culture is defined as "a nation's traditions, values, attitudes, patterns of behaviour, symbols, achievements and particular ways of adapting to the environment and solving problems with respect to the threat or use of force." Booth explained that, while at the general level strategic culture is a result of a nation's history, geography, and political culture, it more specifically represents an aggregation of "the attitudes and patterns of behaviour of the most influential voices," which usually include political elites, military establishments, and public opinion.[56] Different states and security communities will have different ways of thinking about the "threat or use of force for political purposes, and of acting strategically" – and these stem from their distinct histories and geographies.[57] While culture cannot be captured directly, evidence of its presence can be found in a community's ideals and in its ideas, which can be detected in its documents and other artefacts and its behaviour.[58]

As this chapter will later show, it is also strategic culture that means that Israel is a threat society, which in turn shapes Israel's response calculus in all domains, including the cyber domain. Strategic culture is a particularly potent influence on societal dispositions in Israel – indeed, Michael Handel wrote that the IDF, which has in Israel sole responsibility for military affairs and strategic thinking (and now also cyber operations), has a powerful influence on "every facet of Israeli life."[59] In

[52] Waltz, 4.
[53] Waltz, 5.
[54] Freilich, 'Israel's National Security Policy', 413–14.
[55] Freilich, 419.
[56] Ken Booth, 'The Concept of Strategic Culture Affirmed', in *Strategic Power: USA/USSR*, ed. C. G. Jacobsen et al. (Basingstoke: Macmillan, 1990), 121.
[57] Colin S. Gray, 'Out of the Wilderness: Prime Time for Strategic Culture', *Comparative Strategy* 26, no. 1 (8 May 2007): 5, https://doi.org/10.1080/01495930701271478.
[58] Gray, 8.
[59] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 562.

Israel it is also common for senior military officers to enter politics and take up senior government positions, meaning that security thinking is directly transplanted from the military into government decision-making.[60] Strategic culture further filters into society due to the existence of compulsory military service.[61] This is not to say that Israeli society is homogenous; rather, it is simply to say that there is a set of ideas, shaped by historical events, that exerts a particularly strong influence on national decision-making and the disposition towards threats and risks, and these ideas are prevalent across Israeli society. Israel's strategic culture is the product of an especially harsh history of political violence, which has profoundly shaped the way in which Israelis perceive and interpret material dangers. According to a 2020 poll by the Israeli Institute for National Security Studies, 84% of Israelis agreed with the following statement: "If someone comes to kill you – kill him first"; 61% of Israelis surveyed believed that "Arabs only understand force."[62] Both statements, as we will see, are reflections of this culture. Let us now turn to investigating the components of strategic culture that create Israel's identity as a threat society.[63]

5.3.1 The siege mentality

The first important component of Israeli strategic culture that builds Israel's threat society identity is the "siege mentality." Sometimes called the "psychology of insecurity" or "ghetto mindset," it formed one of the guiding beliefs of Zionist ideology and has ever since exerted a strong impact on the Israeli approach to national security.[64] It refers to the belief of a collective that the world is largely hostile towards it and other nations cannot be counted on for help in case of disaster, which leads to an assumption that the collective is subjected to constant existential threat.[65] It thus manifests in a sense of loneliness, self-reliance, and increased sensitivity to threats of annihilation, such as those professed by Iranian leaders.[66] Recall from Chapter 2 that a sense of self-reliance is one of the main features of a threat society. In Israel, these beliefs follow from the Jewish population's long history of persecution and near extermination, life in the diaspora for nearly two millennia, and the collective memory of the

[60] Handel, 555.
[61] Author interview with Eviatar Matania, 17 January 2021.
[62] Zipi Israeli, 'National Security Index Public Opinion Study 2019-2020', INSS, 2020, https://bit.ly/3r3wDh4.
[63] Recall from Chapter 2 that the main features of a threat society are: the willingness to accept risks, the preoccupation with imminent survival threats, and swift reactivity.
[64] Daniel Bar-Tal and Dikla Antebi, 'Siege Mentality in Israel', *International Journal of Intercultural Relations* 16, no. 3 (1 June 1992): 256, https://doi.org/10.1016/0147-1767(92)90052-V; Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 542–43; Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, California: Stanford University Press, 2010), 115.
[65] Bar-Tal and Antebi, 'Siege Mentality in Israel', 253; Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 115.
[66] Bar-Tal and Antebi, 'Siege Mentality in Israel', 253; Freilich, 'Israel's National Security Policy', 416.

trauma of the Holocaust.[67] In more recent history, the siege mentality was reinforced by the surprise attack by the Arab states in 1973, which triggered the Yom Kippur war that continues to haunt Israeli national memory, serving as a reminder that Israeli military dominance over Arab states can never guarantee security.[68] Despite many generations of Israelis having been born in an independent Jewish state and despite the enormous military support provided to Israel by the United States, the siege mentality and pursuit of self-reliance persists, introducing perceptual distortions of material reality. It is continually reflected in Israeli popular and political culture, where the enhancement of security and the struggle for survival are central social values and the IDF is seen as the sole guarantor of the state's continued existence.[69] The siege mentality therefore leads Israeli society to maintain an almost myopic focus on a single, well-defined adversary, which is perceived to threaten its existence. By focusing national attention on a perceived existential threat, the siege mentality is one of the main reasons why Israel is a threat society and emphasises self-reliance as part of "total defence" military planning.[70]

The siege mentality thus intensifies the Israeli perception of Iran as a particularly menacing security threat, even despite the lack of territorial disputes between the two countries.[71] Indeed, Israel currently sees most, if not all, of its regional tensions through the prism of Iran.[72] "If you look at the conflict between Israel and Syria it is partly an Iranian issue. And the conflict between Iran and Hezbollah is also an Iranian issue. The attack of Iranians on Saudi refineries in Jeddah is also part of the Israeli-Iranian conflict," listed Siboni.[73] "Iranian aspirations of hegemony over the Middle East" are viewed as a threat to Israel's existence.[74]

Benjamin Netanyahu, Israel's longest-serving prime minister, many times portrayed the Iranian threat, especially the country's nuclear ambitions, as starkly existential: "[t]here is no moderation in Iran. It is unrepentant, unreformed, it calls for Israel's eradication … " and, "I will never allow Iran to

---

[67] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 542.
[68] Itai Shapira, 'Israeli National Intelligence Culture and the Response to COVID-19', War on the Rocks, 12 November 2020, https://warontherocks.com/2020/11/israeli-national-intelligence-culture-and-the-response-to-covid-19/.
[69] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 543; Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 115.
[70] Total defence is defined as "a security approach involving all of society, under the democratic control of political authorities, and through an institutional collaboration between these authorities, the armed forces, civil administrations, the private sector and the public. It aims to deter a potential enemy by increasing the cost of an attack and reducing its chances of success." See: Joelle Garriaud Maylam, 'Committee on the Civil Dimension of Security: Enhancing the Resilience of Allied Societies Through Civil Preparedness' (Brussels, Belgium: NATO Parliamentary Assembly, 3 March 2021), 2.
[71] Kaye, Nader, and Roshan, *Israel and Iran*, 19.
[72] Kaye, Nader, and Roshan, 19; Merom, 'Israeli Perceptions of the Iranian Nuclear Threat', 93.
[73] Author interview with Gabi Siboni.
[74] Gadi Eisenkot and Gabi Siboni, 'The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran's Malign Regional Influence', The Washington Institute, 4 September 2019, https://www.washingtoninstitute.org/policy-analysis/campaign-between-wars-how-israel-rethought-its-strategy-counter-irans-malign.

obtain the nuclear capability to carry out its genocidal goal of eliminating Israel.[75] Netanyahu's view is not completely unsubstantiated: Iranian supreme leader Ayatollah Ali Khamenei has repeatedly called for Israel's annihilation.[76] It is the Iranian regime's rejection of Israel's right to exist and its identification with the Palestinian cause, which originates in revolutionary dogma, that dredges most deeply into Israel's fears of annihilation and the siege mentality.[77] Indeed, Iran's approach towards Israel has been one of the most uncompromising policies of the Islamic Republic since it came to power in 1979.[78] Its anti-Israel rhetoric functions as a tool for garnering appeal among Sunni Muslims and enhancing its credentials as a major regional power.[79] The Iranian regime's founder, Ayatollah Ruhollah Khomeini, fiercely promoted anti-Semitic views, seeing Jews as agents of western imperialism and as bearing responsibility for the displacement of Palestinian Muslims.[80] Iran's Israel policy is thus a rare example of dogmatic endurance; in many other cases, such as the Russian war against Chechens and China's persecution of Uighurs, Iran abandoned ideological revolutionary convictions once these contradicted the economic and diplomatic interests of the state, showcasing a pragmatic attitude.[81] Further divergences between rhetoric and action were apparent in Iran's decision not to close the Strait of Hormuz, in spite of threats to do so, after an oil embargo put in place by the EU in January 2012.[82]

The Iranian regime has also been vocal in its efforts to deny the Holocaust – for example, former Iranian President Mahmoud Ahmadinejad called it a "lie and a mythical claim."[83] As a result, Israelis, particularly Netanyahu himself, have framed the Iranian nuclear threat in the context of the Holocaust and learning lessons from the past.[84] "The last century has taught us that when a radical regime with global ambitions gets awesome power, sooner or later, its appetite for aggression knows no bounds … The world may have forgotten that lesson. The Jewish people have not," he remarked in front of the UN General Assembly.[85] For Israel, what it perceives as a lack of decisive reaction to Iran

---

[75] Josh Levs, 'Iran Leader's Call to "annihilate" Israel Sparks Fury', CNN, 10 November 2014, https://www.cnn.com/2014/11/10/world/meast/iran-annihilate-israel/index.html; Patrick Kingsley, David E. Sanger, and Farnaz Fassihi, 'After Nuclear Site Blackout, Thunder From Iran, and Silence From U.S.', *The New York Times*, 12 April 2021, sec. World, https://www.nytimes.com/2021/04/12/world/middleeast/iran-israel-nuclear-site.html.

[76] Levs, 'Iran Leader's Call to "annihilate" Israel Sparks Fury'.

[77] David Menashri, 'Iran, Israel and the Middle East Conflict', *Israel Affairs* 12, no. 1 (1 January 2006): 109, https://doi.org/10.1080/13537120500381901.

[78] Menashri, 109.

[79] Reuel Marc Gerecht and Ray Takeyh, 'Iran's Holocaust Denial Is Part of a Malevolent Strategy', *Washington Post*, 27 May 2016, sec. Opinions, https://www.washingtonpost.com/opinions/irans-holocaust-denial-is-part-of-a-malevolent-strategy/2016/05/27/312cbc48-2374-11e6-aa84-42391ba52c91_story.html; David Menashri, *Post-Revolutionary Politics in Iran: Religion, Society and Power* (London: Frank Cass, 2001), 281.

[80] Gerecht and Takeyh, 'Iran's Holocaust Denial Is Part of a Malevolent Strategy'.

[81] Menashri, *Post-Revolutionary Politics in Iran*, 281–82.

[82] Waltz, 'Why Iran Should Get the Bomb', 4.

[83] United States Holocaust Memorial Museum, 'Press Guide to Holocaust Denial in Iran', accessed 28 January 2021, https://www.ushmm.org/information/press/press-kits/press-guide-to-holocaust-denial-in-iran.

[84] Merom, 'Israeli Perceptions of the Iranian Nuclear Threat', 94–95; Kaye, Nader, and Roshan, *Israel and Iran*, 34.

[85] Israel Ministry of Foreign Affairs, 'PM Netanyahu Addresses UN General Assembly 1 Oct 2013', Israel Ministry of Foreign Affairs, 1 October 2013, https://mfa.gov.il/MFA/PressRoom/2013/Pages/PM-Netanyahu-addresses-UN-General-Assembly-1-Oct-2013.aspx.

by other western countries is reminiscent of appeasement,[86] which plays directly into the sense of self-reliance and loneliness that is inherent to the siege mentality.[87]

Israelis also see a link between Iran's ideological anti-Israel stance and the prospect of a nuclear attack.[88] Without exception, all the interviewees for this project affirmed that Israelis "live in existential threat."[89] Harel Menashri, one of the founders of Israel's National Information Security Authority, explicitly linked the collective trauma of the Holocaust to Israelis' understanding of the current security environment:

> We constantly carry with us the memory of the Holocaust and anti-Semitism, alongside the fact that we are surrounded by enemies who want to destroy us, and therefore our culture holds an existential need that is accompanied by a sense of fear and horror to the point of knowing we must always be strong on some levels. … I, for example, spent most of the first nine years of my life in a shelter, under constant attacks on the area where I grew up on a kibbutz in northeastern Israel. It's a personality designer [*sic*].[90]

Expressing similar sentiments, Eviatar Matania, the former Director General of the Israel National Cyber Security Directorate, explained: "[t]here are states that want to destroy us and eliminate us. *It is not just territory*. This is something that *we have felt* from the very beginning, from our independence; it is something that escorts us. It has become part of our culture and strategic thinking that *they want to eliminate, to destroy, to kill us all* [emphasis added]."[91]

When the international community showed some willingness to negotiate with Iran, Netanyahu maintained that "not everyone is constrained by the calculus of cost and benefit that has been associated with nuclear weapons … [therefore] [w]e must not allow the world's most dangerous regimes to possess the world's most dangerous weapon."[92] The powerful prism of historical experience and deeply engrained beliefs about the enduring enmity of its neighbours, combined with the realities of Israel's challenging geostrategic situation and Iran's ideological hostility towards Israel, produces a society that is culturally predisposed to assume the worst of potential challengers and feels continually under threat from a specific adversary.[93] According to Yuval Bazak, the former Head of the Doctrine and Training Department at the IDF, "[i]n Israel now we have again this Iranian threat with all its proxies and

---

[86] For example, after Iran breached the terms of the 2015 nuclear agreement and the European Union decided not to formally accuse Iran of violating the deal, Netanyahu commented that the EU response reminded him of "European appeasement of the 1930s." See: Reuters Staff, 'Israel Says EU's Response on Iran Recalls Nazi Appeasement', *Reuters*, 15 July 2019, https://www.reuters.com/article/us-mideast-iran-eu-israel-idUSKCN1UA1W6.
[87] Merom, 'Israeli Perceptions of the Iranian Nuclear Threat', 96.
[88] Kaye, Nader, and Roshan, *Israel and Iran*, 32.
[89] Author interviews with various Israeli officials, winter 2021.
[90] Author interview with Harel Menashri, 2 September 2020.
[91] Author interview with Eviatar Matania.
[92] 'A Conversation with Benjamin Netanyahu', Council on Foreign Relations, 8 July 2010, https://www.cfr.org/event/conversation-benjamin-netanyahu.
[93] Freilich, 'Israel's National Security Policy', 414–15.

ideology … I think that the public opinion has no doubt. You cannot negotiate with them; you have to confront them. And I think in a way it creates the freedom of decision for decision-makers."[94]

5.3.2 The problem-solving attitude

A second characteristic of Israeli strategic culture, to which the siege mentality contributes, is an "orientation towards doing" and a focus on solving current security problems, which translates into swift reactivity, further enhancing Israel's threat society profile.[95] According to Bazak, "… we have been at war for almost 73 years. Whenever you are at war, you give more attention to the ongoing. You don't think about 2030 or 2040, you think much more about the 'now'."[96] A former senior official from the Israel National Cyber Directorate added: "[w]e suffered upon history a lot and we are survivors. Whoever is left in Israel is a survivor of something. And survivors in most cases are very strong and agile … Israelis are [therefore] very fast minded and learn really quickly and don't have any patience."[97] In other words, Israeli strategic mentality has a "subliminal predisposition … towards decision."[98]

The focus on the present is also informed by the prevailing assumption, drawn from Israel's historical experience, that political violence never stops entirely and will occasionally intensify.[99] The roots of such a belief go back to David Ben Gurion, Israel's first prime minister, who wrote in 1955 that "… [w]e can never assume we can deliver one final blow to the enemy that will be our last battle, after which there will never be a need for another clash or that the danger of war will be eliminated."[100] The belief endured, even as Israel's geopolitical situation changed and it won decisive wars against the Arab states, for example in the 1967 Six Day War, because Israelis continually saw their country as being besieged by adversaries and in a perpetually weaker position due to its small territory – Israel, according to this view, could not afford to lose even a single battle.[101] Israeli decision-makers thus espouse a mission-based mindset and feel under pressure to constantly strive for advantages over the enemy.[102] "We never see problems at a distance but as a result we have learned to react very rapidly when the problem is in front of us," according to Yuval Bazak.[103] Israeli decision-making is therefore highly pragmatic and in military affairs often "doing comes before understanding." Improvisation and

[94] Author interview with Yuval Bazak, 7 January 2021.
[95] Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 111–16.
[96] Author interview with Yuval Bazak.
[97] Author interview with former senior executive at the Israel National Cyber Directorate.
[98] Dmitry (Dima) Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', *Security Studies* 26, no. 1 (2 January 2017): 175, https://doi.org/10.1080/09636412.2017.1243923.
[99] Thomas Rid, 'Deterrence beyond the State: The Israeli Experience', *Contemporary Security Policy* 33, no. 1 (1 April 2012): 134, https://doi.org/10.1080/13523260.2012.659593.
[100] Ben Gurion cited in: Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 537.
[101] Adamsky, 'From Israel with Deterrence', 165.
[102] Author interview with Yuval Bazak; Author interviews with various Israeli officials.
[103] Author interview with Yuval Bazak.

creativity are encouraged as these allow for greater flexibility in crises and assist the mission for survival.[104]

Israel's cultural predisposition towards swift and decisive reaction as a threat society means that, unlike in the case of risk societies, the potential unintended side effects of its own decisions do not inhibit action. Israel, in other words, is not reflexive; rather, the focus of policymaking is on addressing present dangers head-on. The fixation on the threat to survival in the form of a clearly defined actor displaces any concerns about blowback or unintended secondary and tertiary effects to a lower priority. There is primarily one catastrophic scenario that dominates Israel's strategic thinking: the prospect of annihilation by a clearly defined adversary – Iran. As Yuval Bazak noted, "[t]hink about what happened to the US or even all of NATO after the USSR collapsed. They started to question: who is our enemy? … We have never had to ask ourselves "who is our enemy", our enemies were always just in front of us. Their intention has been very clear."[105]

5.3.3. The cult of the offense

The historical presence of a clearly defined enemy, always perceived to be bent on Israel's destruction, in addition to creating the problem-solving attitude and the adaptive mindset described above, also led to the "cult of the offense" – a third important characteristic of Israeli strategic culture. Like the previous two characteristics, the cult of the offense creates Israel's threat society identity – this time, by encouraging risk-acceptant behaviour in relation to hostile foreign actions.

The concept of the cult of the offense means a "politico-military belief that offense will be victorious under any circumstances," which "predisposes states to attack their adversary."[106] The term has previously been used in IR literature to explain the origins of the First World War.[107] In Israel, the association of defensive warfare with the victim mentality of the Diaspora Jews meant that offensive strategy has long been viewed as a superior form of warfare, more in tune with the dynamism, initiative, and improvisation that characterises Israeli society.[108] The Israeli security community also believes in the "ethos of excessive attack," which is firmly built into Israel's military doctrine (later we will see its resonance in the notion of disproportionate retaliation).[109]

---

[104] Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 117.
[105] Author interview with Yuval Bazak.
[106] Adamsky, 'From Israel with Deterrence', 166.
[107] See: Stephen Van Evera, 'The Cult of the Offensive and the Origins of the First World War', *International Security* 9, no. 1 (1984): 58–107, https://doi.org/10.2307/2538636; Jack Snyder, 'Civil-Military Relations and the Cult of the Offensive, 1914 and 1984', *International Security* 9, no. 1 (1984): 108–46, https://doi.org/10.2307/2538637.
[108] Adamsky, 'From Israel with Deterrence', 166.
[109] Adamsky, 166.

The origins of this offensive approach, as in the case of the problem-solving attitude, lie in the sense of an ever-present enemy, combined with the observation that Israel lacks strategic depth.[110] What's more, Israeli "offensive romanticism" has not waned during the course of history, even after the aforementioned 1967 Six Day War when Israel acquired some strategic depth.[111] As a result, in Israel, military solutions such as reprisal raids are often selected as a first resort, rather than a last resort option.[112] In its cult of the offense, Israel also established a distinct preference for deterrence by punishment over deterrence by denial, with significant implications, as we will see, for how the country addresses cyber attacks.[113] On the whole, a strong belief in the superiority of offensive action has meant that Israel is a risk-taker. Indeed, the IDF even discusses risk-taking as a necessary part of its deterrence doctrine.[114]

5.4 The influence of the threat society on Israel's deterrence strategy and responses to cyber attacks

Having discussed the three features of strategic culture that form Israel's threat society identity, we now move on to discussing Israel's deterrence strategy and contextualising and explaining Israeli responses to cyber attacks through the prism of the threat society. In Israel, unlike in many other countries where signals intelligence agencies separate from the military contribute to national cyber defence, signals intelligence falls under the purview of the IDF. Consequently, the IDF is also responsible for responding to state level cyber attacks, leaving responses similarly susceptible to strategic cultural influences.[115] First, we will discuss Israel's conventional deterrence strategy. Here it is important to note that Israel's deterrence thinking was not the result of a material considerations alone. Instead, Israel's deterrence posture, developed over the course of many years of often violent confrontation with different adversaries, was also built on the features of the threat society discussed above. Second, we will consider how Israel transplanted conventional deterrence thinking into the cyber domain and also fitted cyber issues into its larger, pre-existing threat society identity. Third, the discussion will move to an analysis of how Israel's perception of Iran (through a threat society lens) led the country to regard cyber conflict as yet another "Iran issue" and how this influenced Israel's

[110] David Tal, 'Israel's Wars', in *The Oxford Handbook of Israeli Politics and Society*, ed. Reuven Y. Hazan et al. (Oxford: Oxford University Press, 2021), 112–13; Author interview with senior military cyber defence official; Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 539.
[111] Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 112–13.
[112] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 555.
[113] Adamsky, 'From Israel with Deterrence', 166.
[114] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces' (Harvard Kennedy School, August 2016), https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf.
[115] Author interview with senior military cyber defence official.

responses to cyber attacks. Finally, the section will end with an analysis of the response to Iran's attack on Israel's water management facilities and illustrate how Israeli conventional deterrence thinking, in combination with its perception of Iran, which were both in themselves products of strategic culture, shaped the Israeli threat society's response.

5.4.1 Israel's conventional deterrence strategy

It is difficult to overemphasise the importance that the Israeli security community attaches to deterrence as a means of preserving the survival of what they see as the besieged Israeli state. As Itai Brun, the former Head of Israel Defense Intelligence (IDI), put it, "Israel is built on deterrence. We feel that we exist because of deterrence, not because of anything else."[116] Israel's conventional deterrence thinking rests on the premise that the *repeated* use of force against enemies will eventually have the effect of changing their future decision calculus of offensive action – leading some scholars to label it "cumulative deterrence."[117] Intrinsic to this approach is the assumption that deterrence will, at times, fail.[118] The goal of Israeli deterrence is thus not the absolute prevention of all political violence – regional antagonisms in the Middle East are perceived by Israel to be such that hostilities and conflict will never be completely avoidable[119] – but rather the postponement of all-out war for as long as possible.[120] Such thinking goes back to the doctrinal principles developed in the 1950s by Ben Gurion – strategic deterrence, early warning, and decisive victory.[121] The purpose of deterrence was to simply elongate the time between wars to allow Israel to rearm.[122] Israel does not so much hope to dissuade the enemy from launching a specific type of attack, but rather, deterrence must be "generalized and

[116] Author interview with Itai Brun, 1 March 2021. Brun was also the Founder and Director of the DADO Center for Interdisciplinary Military Studies, the IDF's internal thinktank.
[117] Adamsky, 'From Israel with Deterrence', 172; Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* 40, no. 1–2 (2017): 102, https://doi.org/10.1080/01402390.2015.1115975.
[118] Dmitry (Dima) Adamsky, 'From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies* 41, no. 1–2 (23 February 2018): 163, https://doi.org/10.1080/01402390.2017.1347872.
[119] Freilich, 'Israel's National Security Policy', 416.
[120] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 93.
[121] Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, 112; Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations', application/pdf (Zürich: ETH Zurich, September 2020), 9, https://doi.org/10.3929/ETHZ-B-000438397; Author interview with senior military cyber defence official; Adamsky, 'From Israel with Deterrence', 162.
[122] If a war was on the horizon, *early warning* of its occurrence was to allow for the deployment of reservists and pre-emptive action; on the battlefield, the aim was *decisive victory* in order to reinvigorate deterrence. Adamsky, 'From Israel with Deterrence', 165; Tal, 'Israel's Wars', 112–13; Author interview with senior military cyber defence official.

cumulative over time in order to maintain the existing situation and frame the 'rules of the game' favourable to Israel."[123]

According to Jonathan Shimshoni, such an approach to deterrence emphasises the centrality of a state's reputation for retaliation – if a state punishes adversaries consistently, over time it will establish a reputation for severe responses, which will eventually result in fewer attacks from adversaries.[124] This highly reactive posture is a product of the threat society. Indeed, Israeli decision-makers believe that declaratory threats alone are insufficient to establish credibility.[125] Instead, explained Matania, "[w]e believe, generally, that deterrence will be mostly a result of our behaviour. We want to shape and structure deterrence based on our activities."[126] The use of force periodically, the execution of the threat of punishment, is necessary in order to develop a "reputation for toughness" and ensure the credibility of future punishment.[127] The 2015 IDF Strategy, Israel's first ever published defence doctrine,[128] espoused the same beliefs – it explained that the first essential component of deterrence is "[a] credible threat of severe offensive operations that will exact a heavy toll if we are attacked."[129] In order to bolster that credibility, Israel engages in "[l]imited offensive actions to signal that the 'rules of the game' have been broken [although, it should be noted, the "rules" are often intentionally ambiguous] and there is a readiness to take risks."[130] This section of the IDF Strategy is also illustrative of another main feature of threat societies: the willingness to take risks. As this chapter already discussed, the predisposition of Israeli strategic mentality towards decision (usually offensive action of some variety), and the belief that Israel can only count on itself, is what undergirds risk tolerance.[131] Offensive responses are signals to the adversary that Israel will not tolerate the activity that provoked the response; they are intended to prove to the adversary that Israel is prepared to inflict severe offensive punishment, regardless of the potential risks, in the case of further attacks.[132]

---

[123] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 24.
[124] Jonathan Shimshoni, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca, NY: Cornell University Press, 1988), 215. As Richard Harknett pointed out, the "less-than-appealing conclusion" of such an approach is that "deterrence may require occasional small wars." Richard J. Harknett, 'The Logic of Conventional Deterrence and the End of the Cold War', *Security Studies* 4, no. 1 (September 1994): 88, https://doi.org/10.1080/09636419409347576.
[125] Adamsky, 'From Israel with Deterrence', 166.
[126] Author interview with Eviatar Matania.
[127] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 93; Adamsky, 'From Israel with Deterrence', 163.
[128] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', 9.
[129] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 25.
[130] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 25.
[131] Adamsky, 'From Israel with Deterrence', 175.
[132] Adamsky, 173.

Another guiding principle in the Israeli approach to deterrence is the idea that it requires a position of perceived superiority over the adversary.[133] In order to do this, consistent with the cult of offensive action, Israeli decision-makers believe that punishment often needs to be more severe than the original attack as this show of force, by imposing high costs, is more likely to convince the adversary that the price of its aggression is too high.[134] "Retaliation has to be non-proportional, otherwise you won't get anywhere," asserted Siboni.[135] On Israel's northern border, explained Brun, a period of quiet ensued only after "the unproportionate response of Israel in 2006 after the kidnapping and killing of our three soldiers."[136]

In sum, Israel's deterrence thinking is the combined product of the strategic cultural elements that form the threat society: the siege mentality indicates that Israel faces ever-present survival threats and adversaries will only understand severe punishment; the problem-solving attitude means that punishment is imposed swiftly and consistently; and the cult of the offense invites a willingness to administer punishment through the use of force, often disproportionate to the original attack. Fundamental to the deterrence strategy is also the willingness to accept risks, particularly the risk of escalation, that can result from severe punishment.

5.4.2 Israel's conventional deterrence strategy in the cyber domain

Unlike in the United States, where deterrence rose to prominence during the Cold War in the context of nuclear weapons, in Israel, deterrence based on reprisals was already employed in practice in conflicts between militant groups prior even to the Israeli state's foundation.[137] It was not a coherent theory developed by a group of strategic thinkers in relation to a particular capability (the atomic bomb), but the product of learnings from common practice, which formed a set of "institutionalized improvisations."[138]

Because Israel's deterrence strategy pertains to all domains of conflict, not just the nuclear one, some scholars believe that the extension of its logic to new domains like cyberspace is natural.[139] And indeed, Israel directly transplanted its conventional deterrence strategy into the context of cyberspace. Like in the physical domain, the goal of Israeli cyber deterrence is not to prevent incidents from occurring altogether. Instead, according to a former senior defence official, "deterrence within cyber is

[133] Adamsky, 166.
[134] Author interview with Itai Brun.
[135] Author interview with Gabi Siboni.
[136] Author interview with Itai Brun.
[137] Rid, 'Deterrence beyond the State', 124.
[138] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 94; Adamsky, 'From Israel with Deterrence', 164.
[139] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 93; Adamsky, 'From Israel with Deterrence', 164.

all about stiffening [the] finger [that presses the button on cyber acts]."[140] Israeli cyber deterrence is therefore more *restrictive* than absolute in nature; the infliction of punishment is meant to be a "learning experience" for the aggressor, which results in past and potential offenders moderating their future behaviour.[141] According to Matania, "[t]he limits and boundaries of cyber attacks are [currently] being shaped. So the way we behave and what we do will shape the whole approach of all players in cyberspace, what is done and what is not done against Israel."[142]

There are three main, interlinked themes that are present in Israel's cyber deterrence thinking: a focus on the attacker (rather than the nature of the operational domain), forceful punishment and the acceptance of escalation risks, and intentional unpredictability and the reservation of a right to a military response. All three of these themes align with conventional deterrence thinking. Like Israel's deterrence thinking, they are the product of Israel's threat society identity.

A) Focus on the attacker (threat)

Consistent with the expectations of the risk framework, in the Israeli threat society, policymakers focused mainly on the perpetrator of a cyber attack (the threat), rather than the domain in which the attack was launched (potential risks). According to Matania, as soon as a cyber attack rises to the level of a national security concern (as opposed to routine cyber crime), the policy focus shifts from the *type of attack* to the *attacker* and "you do everything which is needed to do in order to retaliate and deter."[143] As we will see, in practice this meant that Israeli policymakers treated any act of Iranian aggression, regardless of its means, as a serious threat to national security.

Israel's intense focus on the attacker, rather than the domain of attack, also permeates the IDF strategy, which makes clear that deterrence must be "specific and adapted to each enemy," particularly to the enemy's "characteristics, considerations, capabilities, identity, and decision-making processes."[144] The importance that Israel attaches to enemy identity is tightly woven with the siege mentality and the belief that adversaries wish to annihilate Israel (the enormous importance that Israel attaches to the enemy's perceived identity will also be illustrated in the next section). Israel's enemy-centric, rather than domain-centric, security focus is therefore another feature that distinguishes it from how risk societies approach cyberspace in terms of the attention they pay to the operational domain and its escalatory potential. It means that Israeli policymakers see no obstacle to transplanting familiar deterrence thinking from the conventional domain to the cyber domain.

[140] Author interview with former senior defence official, February 2021.
[141] Rid, 'Deterrence beyond the State', 128; Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 93.
[142] Author interview with Eviatar Matania.
[143] Author interview with Eviatar Matania.
[144] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 24.

B) Forceful punishment and acceptance of escalation risks

Israeli decision-makers believe that cyber attacks, even ones that do not result in death or severe destruction, should be met with forceful punishment. A history of extended friction with Palestine and with Hezbollah on Israel's northern border has over the last few decades eroded Israel's willingness to weather any kind of attacks, including cyber attacks, without reacting forcefully.[145] For example, in the kinetic domain, despite the existence of the "Iron Dome," a sophisticated air defence system, Israel employs "attacking back" as part of its defence strategy.[146] Matania emphasised that, regardless of the domain in which the attack is launched, the adversary "must know that we are going to react. They must know that they cannot just attack us."[147] There is a sense among policymakers that permitting even a minimal shift in the status quo would be incredibly detrimental to Israeli security.[148] Similarly, in the cyber domain Israeli security officials believe that they cannot solely rely on passive defence to protect Israel's digital terrain; the country must also retaliate. Neglecting the ability to retaliate for cyber attacks, according to a former senior defence official, is the same as "governments that in the 1920s did not believe in creating your own air combat power."[149] Israeli policymakers thus transplanted strategic thinking directly from the kinetic domain into the cyber domain.

Israeli decisionmakers also engage in what Rid called "utilitarian" justifications for punishment, as opposed to "retributive" ones. The former are forward-looking and geared towards the wider social benefits of punishment, such as more regularised behavioural patterns and a reduction in offensive actions, as opposed to the latter whose focus is the infliction of proportional pain "because the offender deserves it." The latter also involves a rejection of the wider social benefits of punishment, including deterrence.[150] An interview with a former Israeli senior defence official affirmed that Israel employs the same thinking in the cyber domain: "… to hit back is not in order to get the satisfaction of punching someone back … [it is] to get the other side to reconsider again and again before using [those] capabilities."[151] It comes as no surprise that Israel as a threat society prioritises a pragmatic attitude towards punishment, including for cyber operations. Recall that Israel's chief concern is long-term survival in the face of an actor that it perceives to be an existential threat. It will not waste time or resources on punishing solely for the purpose of retribution (nor will a risk society for that matter – though for different reasons, prioritising primarily the possibility of unintended effects). Deterrence through punishment, in helping create and enforce *de facto* norms of behaviour,[152] for Israel offers a tool for helping ensure society's survival.

[145] Author interview with Daniel Moore, 25 January 2021.
[146] Author interview with Eviatar Matania.
[147] Author interview with Eviatar Matania.
[148] Author interview with Daniel Moore.
[149] Author interview with former senior defence official.
[150] Rid, 'Deterrence beyond the State', 128.
[151] Author interview with former senior defence official.
[152] Rid, 'Deterrence beyond the State', 129.

The question that naturally arises here is whether forceful punishment for a cyber operation risks unintentionally escalating a cyber conflict, a concern which, as Chapter 4 showed, featured prominently in the US risk society. "I will tell you something about our neighbourhood," answered Matania, "we know that if it can escalate, it will escalate, regardless of what we do. And sometimes it is better that you escalate before they escalate or you do something which is not proportional."[153] Another senior military cyber defence official admitted, "talking about escalation in the cyber domain is a bit weird for me." "Because escalation is escalation. You can hit me with a missile and I will hit you back with a platoon … Working in the cyber domain, there is no point being worried about escalation. Escalation could come from anywhere."[154]

Israel, in short, characteristically of a threat society, accepts the risks of escalation, whether in cyberspace or in other domains. As Chapters 2 and 3 discussed, a threat society will tend to be less preoccupied than risk societies with the unintended effects of their own actions – in the case of Israel, it is an existential threat in the form of a clearly defined actor that dominates its perception of the security landscape, relegating risks like unintended cyber escalation to a far lower priority. As one senior official admitted, often decisions to act fast are also made without thinking them through; at the root of such tendencies lies the fear, developed over decades of political conflict, that, "[i]f you think about it too much, you will likely die."[155] Once again, this kind of reasoning is typical of a threat society, which evaluates decisions primarily through the prism of potential annihilation by an ideological enemy. Decisions are thus guided by a universal paradigm, reinforced over decades of exposure to existential violence, that weak action leads to defeat and destruction.

C) Intentional unpredictability and the right to a military response

The Israeli approach to deterrence, focused on implementing punishing actions rather than issuing threats of action, means that Israeli decisionmakers are reluctant to draw exact red lines and make public commitments to how and when they will react to cyber incidents – the objective instead is to preserve the flexibility of response and not provide the adversary with any margin for manipulation (as we already discussed, Israel's main deterrence objective is to create a reputation for retaliation).[156] Additionally, Matania explained that in order to deter adversary activity effectively in the Middle East, it is important to instil in the adversary a sense that you may act irrationally and unexpectedly, much like playing a "game of chicken."[157] Or in the words of General Gadi Eizenkot, the former IDF Chief

[153] Author interview with Eviatar Matania.
[154] Author interview with senior military cyber defence official.
[155] Author interview with senior government official, January 2021.
[156] Author interview with Eviatar Matania; Author interview with Daniel Moore.
[157] Author interview with Eviatar Matania.

of General Staff: "[a]nother interest is to … maintain the deterrence and the image and capability of the IDF as an unpredictable enemy that can react in a very severe way."[158]

The lack of discussion of how Israel will respond to specific attacks, and, within this, cyber operations, in official Israeli doctrine is in line with the general attitude of the Israeli leadership, which holds back from disclosing declaratory policy in public documents (Israel for example still does not have a formal national security strategy).[159] This attitude can be seen as an extension of the desire to maintain a reputation for unpredictable, but forceful responses. "We believe that if you want to shoot - shoot, don't talk," professed Matania. "That's why we don't talk much about [our response strategy]."[160] The desire to preserve some unpredictability, and even a sense of irrationality, in responses, alongside the desire to develop a reputation for forceful retaliation, led Rid to point out that the Israeli strategy contains certain contradictions – the Israeli leadership wants to seem unreasonable and predictable at the same time.[161] One way of understanding this thinking is to draw a distinction between the macro level and the micro level: on a macro level, Israel wants to establish a reputation as a tough punisher, while on a micro level, it wants to instil in the adversary the uncertainty as to exactly how an attack will be punished.

An extension of this nuanced strategy is the assertion that a cyber attack need not necessarily be met with a cyber response. Yigal Unna, for example, publicly stated that "[w]e have the ability to respond powerfully against cyberattackers, and not necessarily in the same space in which they attacked."[162] "I will retaliate back the way I want and where I want," reaffirmed a cyber defence official in an interview.[163] What is distinctive about these Israeli assertions is their implication that Israel reserves the right to use *military force* to respond to a cyber attack, regardless of whether the initial attack met the use of force threshold. In Israel, reserving the right to respond in a different domain therefore translates directly into keeping a kinetic strike as an option on the proverbial table. Israel wants its adversaries to know that it will respond forcefully to any attack, regardless of the attack's means.[164] Such a threat was substantiated by Israeli practice: as we discussed earlier, Israel responded to an alleged cyber operation by Hamas with a military strike on its cyber unit.[165]

Maintaining as an option a military response to a cyber operation is consistent with Israel's threat society identity and emerged as a consequence of the cult of the offense and the desire to solve

---

[158] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 25.
[159] Lior Tabansky and Isaac Ben-Israel, *Cybersecurity in Israel* (Cham: Springer International Publishing, 2015), 4; Freilich, 'Israel's National Security Policy', 1.
[160] Author interview with Eviatar Matania.
[161] Rid, 'Deterrence beyond the State', 143.
[162] Yigal Unna cited in: Siman-Tov and Even, 'A New Level in the Cyber War between Israel and Iran'.
[163] Author interview with senior military cyber defence official.
[164] Author interview with Daniel Moore; Author interview with Eviatar Matania.
[165] Israel Defense Forces (IDF), 'CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets.'

problems quickly. Issuing a military strike in response to a cyber attack was also born from the idea that problems must be dealt with while they are still small, which is a lesson learned through history. The senior cyber defence official, citing the example of Hamas' increased militarisation in the Gaza Strip and Iran's increasing influence in Syria, explained that, "every time we make the mistake of letting something go, we pay the price."[166] Despite the fact that "cyber is not bleeding yet," he continued, these "lessons learned" from recent history meant that Israel started thinking about cyberspace as a military operational domain early and adopted the mentality of not letting adversaries "get away with" hostile cyber incidents.[167]

Finally, it is important to mention that the Israeli belief in the need to respond forcefully to cyber attacks does not preclude Israel's engagement in preventive action. According to one official, Israel generally employs "offensive thinking" to cyber issues, which includes both responses and pre-emption or prevention: "[i]f possible, I am not going to wait until the malware becomes a problem. I am going to foil it before."[168] We will return to Israeli preventive action in section 5.5 when we discuss the campaign between wars.

5.4.3 Cyber conflict as another "Iran issue"

In the last section, we discussed how Israel's threat society identity leads it to focus intensely on the perpetrator of an attack, rather than the means used or the operational environment, which allowed it to transplant conventional deterrence thinking directly into the cyber domain. The chapter also previously discussed how Iran treads particularly on Israeli sensitivities rooted in the collective trauma of the Holocaust, which intensifies the threat-based prism through which Israel perceives its own security position and makes security-related decisions. This section elaborates on how Israel's threat society fixation on Iran meant that cyber conflict, rather than being seen as a distinct strategic arena of general interstate competition, came to be viewed through the prism first and foremost of "the Iranian issue," much like all other issues of national security.[169] As Itai Brun put it, "[w]e are fighting Iran. Part of this fighting is being done kinetically, part of it is being done in the cyber domain. For us, the issue is the war, it's not the domain. We have this comprehensive view of the battlefields. And the cyber domain is another battlefield."[170]

Iran, Hezbollah and Hamas are perceived to be rapidly improving their cyber capabilities. According to Yigal Unna, "Iran and its proxies remain the main cyber threat in the Middle East."[171] What's interesting is that Iranian cyber capabilities are, in fact, not likely to be particularly

[166] Author interview with senior military cyber defence official.
[167] Author interview with senior military cyber defence official.
[168] Author interview with senior military cyber defence official.
[169] Author interview with Gabi Siboni.
[170] Author interview with Itai Brun.
[171] Yigal Unna cited in Siman-Tov and Even, 'A New Level in the Cyber War between Israel and Iran'.

sophisticated. The failure of the attack on the water infrastructure in 2020 is one example. According to Daniel Moore, a private sector threat intelligence engineer (and former IDF member) who tracks advanced persistent threat (APT) actors, "[the Iranians'] ability to enact large-scale, effective, and harmful operations against critical infrastructure on any meaningful scale beyond wiper malware is something that is entirely unproven … their ability to cause harm is not proportional to what the US, Israel, the UK can do. It's a different tier of threat actor."[172]

Because Iran is regarded as Israel's primary existential threat, however, the Israeli security community finds the prospect of Iran "getting away with" attacking *anything* completely unacceptable.[173] "We can't allow them to develop cyber capabilities," stipulated the senior cyber defence official, "It's like a biological weapon. You can't just be like 'they only went after an insurance company'. Tomorrow they will go after a dam."[174] Such an approach might be described as "not yielding an inch" to Iran; regardless of whether the effects of an Iranian operation are serious, because of the "sense of existential dread" that Iran provokes in Israel,[175] any Iranian aggression warrants immediate retaliation. According to Isaac Ben-Israel, a former general who founded Israel's National Cyber Bureau at the Prime Minister's Office and formulated Israel's first cyber policy, although Iran may not be the most cyber capable country in the world, "there is a difference here because the Iranians, whatever they do, even if it's not first grade technology, they do it in order to harm Israel."[176] Israel perceives its margin of error with Iran to be much smaller than that of other countries vis-à-vis their adversaries; responses to any Iranian aggression, even non-violent attacks, are powerful because Israelis want to "aggressively shut down any notion that something like [cyber operations] could work [for Iran]."[177]

According to the former INCD executive, the cultural and ideological feature of the animosity between Israel and Iran makes this relationship distinctive from, for example, the United States' relationship with Russia.[178] Siboni was more direct: communication with Iran and its proxies is "best understood when it is kinetic."[179] Thus, regardless of the means that Iran employs, Israeli policymakers fall back on the same frames of reference. Matania summarised the continuity between Israeli strategic thinking in the physical domain and in cyberspace using the following analogy:

> We always play between Athens and Sparta. We are Athens inside (liberalism and culture and technology etc.) and Sparta when it comes to our neighbours and security. And it is the same when it comes to the cyber domain.

[172] Author interview with Daniel Moore. For further discussion of Iranian and Iranian-linked operations against Israel see: Work and Harknett, 'Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges', 5–7.
[173] Author interview with Daniel Moore.
[174] Author interview with senior military cyber defence official.
[175] Author interview with Daniel Moore.
[176] Author interview with Isaac Ben-Israel, 27 January 2021.
[177] Author interview with Daniel Moore.
[178] Author interview with former senior executive at the Israel National Cyber Directorate.
[179] Author interview with Gabi Siboni.

On the one hand, we want to develop new technologies and export them, but when it comes to threats to Israel and security, we act the same way as we do everywhere else. We are Sparta.[180]

Viewing cyber conflict through the prism of the Iranian threat also has implications for how Israel approaches attribution – which, as we explored in Chapter 3, is often seen as a difficult endeavour in the cyber domain. Roy Schondorf, Israel's Deputy Attorney General, in explaining Israel's position on attribution, acknowledged what this thesis considers to be the concerns of risk societies: "[s]ome have suggested that there needs to be more legal certainty with respect to attribution, in order to avoid mistaken attribution, which can lead to conflict escalation." According to his perspective, however, such concerns are largely a "theoretical issue," whereas attribution is at its essence "a technical matter" – consequently, Schondorf advised "against over-regulating the issue."[181]

Israel has never engaged in the practice of publicly attributing cyber attacks, collective or otherwise. Israeli policymakers do not see the *difficulty* of attribution as a fundamental challenge that could pose an obstacle to issuing a meaningful response to a cyber operation. In fact, quite the opposite: rather than being regarded as an essential step that legitimises a later response and helps avoid unwanted escalation, the public announcement of an attribution statement can, according to Israel, impede the application of a meaningful response. Announcing a cyber response in advance could, according to Schondorf, "negate its utility and effectiveness, and in some instances undermine the interests of the injured State" as "the other side may thwart the action if it anticipates it."[182] Fundamentally, Israel's primary concern is to be able to retaliate swiftly and forcefully against Iranian aggression, cyber or otherwise. Cyber retaliation is not viewed through the prism of its associated risks – it is viewed, like any other capability, on its merits as a tool of retaliation in a particular situation. By swiftly punishing an attack, Israel signals to the adversary that it has attributed the operation and fortifies its reputation as an uncompromising retaliator.

Another factor that contributes to Israel's view that public attribution is unnecessary, and can even be damaging, is that Israel does not doubt the sponsor of the attacks. According to Siboni, "you know who attacked you. You don't have to go to court to prove it [or] … provide hardcore evidence. … You retaliate because you know who did it."[183] In this sense, because Israel's security issues are linked to one specific threat actor, Israel sees the universe of potential perpetrators and sponsors of cyber attacks as being substantially narrower.[184]

---

[180] Author interview with Eviatar Matania.
[181] Roy Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL: Talk!* (blog), 9 December 2020, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.
[182] Schondorf.
[183] Author interview with Gabi Siboni.
[184] Although one might question the extent of Iran's direct involvement in an attack that comes from Hamas or Hezbollah, for Israel, attacks coming from Hamas and Hezbollah will nevertheless be seen as part of the wider regional conflict with Iran.

Now that we have established the cultural threat society framework through which Israel addresses security issues, cyber conflict, and responses to cyber attacks, the following section will apply the framework to understand Israel's response to the 2020 cyber attack on its water infrastructure.

5.4.4 Israel's response to Iran's water system attack

Israel's reaction to the Iranian attack on its water infrastructure in 2020 illustrates the influence of Israel's threat society identity on responses to cyber attacks. First, the view of Iran as an existential threat permeated the interpretation of the attack itself. According to one interviewee, the Iranians had signalled that they can "reach every tap in Israel" and "frighte[n] the needs of a wide civilian population."[185] Speaking in May 2020, in the direct aftermath of the attack, Yigal Unna cautioned that the operation was "designed to trigger a humanitarian disaster" and thus marked a turning point in the "history of modern cyberwars."[186] The attack on the water infrastructure was not only a reconnaissance operation, according to a former senior defence official, rather, it was like a "bunch of parachuters, a commander unit, getting into critical assets and waiting to be called … It was one level under nuclear capabilities."[187] Had Israel not responded, Israelis believed, this would have further emboldened Iran.[188] Dmitri Alperovitch, a well-known cybersecurity professional and co-founder of cybersecurity firm CrowdStrike, reasoned that Israel's response to Iran's cyber interference in its water treatment facilities was in line with existing Israeli policy of responding aggressively to Iranian provocation. "Any time you see Iranian escalation, as with their build-up of rocket capacity in Syria, you have consistently seen Israeli retaliation with bombing runs on those positions. So it appears they have now applied that doctrine in cyberspace."[189]

Second, in devising the response, a cyber attack on Iran's Shahid Rajaee port, Israel implemented conventional deterrence thinking, which, as we discussed earlier, is also shaped by Israel's threat society identity. According to a former senior defence official, the message that Israel sent through the attack on Shahid Rajaee port was the following: "[y]ou didn't create any damage, you just planted the seed that would allow you to later take aim at us. But there will be a price for every act like that and the price is going to be severe."[190] While the damage done to the port was temporary and did not result in any deaths, "it was a very painful message that was aimed to warn, to embarrass, to punish,

[185] Author interview with former senior defence official.
[186] Yigal Unna cited in Inon Ben Shushan, '"Failed Cyber Attack on Israel Was Designed to Trigger a Humanitarian Disaster"', JNS.org, 31 May 2020, https://www.jns.org/failed-cyberattack-on-israel-was-designed-to-trigger-a-humanitarian-disaster/.
[187] Author interview with former senior defence official.
[188] Author interview with former senior defence official.
[189] Alperovitch cited in: Warrick and Nakashima, 'Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran'.
[190] Author interview with former senior defence official.

and to collect a price from the threat actor. That's deterrence."[191] Itai Brun concurred: "the idea was … some kind of unproportional response, which is something rooted in Israeli thinking. The issue of the price vis-à-vis the action; [here] the penalty is very important. That we are doing something that is much bigger, heavier, more painful than the other side [*sic*]."[192] Indeed, according to Ben-Israel, the response was designed to warn Iran, "don't start playing with this type of warfare because I'm much stronger and I can cause much bigger damage than you."[193] The intention was, added Bazak, to "reduce [their] willingness to go into this kind of fighting."[194]

As the earlier discussion in the chapter showed, Israel aims to deter adversaries primarily by establishing a reputation as a forceful retaliator, which is again a result of being a highly reactive threat society. The cultural belief in the superiority of offensive action, coupled with the siege mentality, means that Israel approaches security issues with the aim of repeatedly demonstrating its capability and willingness to inflict unacceptable costs on the adversary, as it believes that ultimately this is the only means of effectively deterring adversaries from endangering Israel's survival. Thus, unpacking the response to the Iranian water attack further, Brun explained that the wider objective of the response was to "signal something much bigger – superiority." According to Brun, and chiming with the earlier observation by Matania that Israel does not seek to establish firm red lines, Israel did not set out to "deter [a] *specific action* by retaliating [emphasis added]." Instead, through the Bandar Abbas attack, "Israel wanted to signal: we are more powerful, more in control, more advanced, while you are exposed." "By building superiority," concluded Brun, "you achieve deterrence."[195]

Finally, it is worth pointing out that although the Israelis chose to respond to the Iranian attack using cyber means, this decision was unlikely to have been guided by the desire to respond in kind. According to Moore, the Israeli operators would have compromised the port long before the attack, which means that the digital disruption of the port had been an existing capability in their arsenal.[196] Thus, in this case, the retaliatory cyber operation was the "most adequate tool in their toolbox" in order to achieve a desired effect: communicating to Iran a powerful deterrent message that attacking Israel would carry consequences, regardless of the domain in which the attack was launched.[197]

Having discussed how Israel's threat society identity, which is in itself a product of strategic culture and historical experience, influenced responses by shaping both deterrence strategies and the

[191] Author interview with former senior defence official.
[192] Author interview with Itai Brun.
[193] Author interview with Isaac Ben-Israel.
[194] Author interview with Yuval Bazak.
[195] Author interview with Itai Brun.
[196] Moore thus called the retaliation a "presence based operation," which involves a long prior network intrusion process during which operators establish themselves on a target's systems: Author interview with Daniel Moore.; For further scholarly analysis of the Shahid Rajaee operation see: Work and Harknett, 'Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges', 4.
[197] Author interview with Yuval Bazak; Author interview with Daniel Moore.

perception of Iran, let us now turn to a discussion of Israeli preventive action, known as the strategy of the campaign between wars, or "mabam."

5.5 Prevention, resilience-building, and consequence management

5.5.1 "Mabam": the campaign between wars

Israel's commitment to meaningful punishment does not preclude preventive action. Israeli strategy in fact combines both individual responses and preventive action for the purposes of deterrence. The country's preventive strategy is carried out under the concept of the campaign between wars (CBW) or "mabam" in Hebrew. As the 2015 IDF Strategy explained, "many of the actions meant to deter will be carried out within the framework of [the] campaign between wars."[198]

The CBW was initially developed around 2013 as a general response to the development of the Islamic Revolutionary Guards Corps Quds Force (IRGCQF) and proxy forces in Syria.[199] At the most basic level, its aim is to employ force to maintain and build upon the gains made during the course of previous conflicts and prevent or delay the next war.[200] Because adversaries use the short periods between conflicts with Israel to "refill their arsenals and evolve their tactics and capabilities," actions under the CBW aim to forcefully prevent adversaries' build-up of advanced capabilities.[201] Having evolved from a special operations logic, it consists of "proactive, offensive actions based on extremely high-quality intelligence and clandestine efforts."[202] One of its guiding principles refers to "[i]nitiated and controlled action below the war threshold for short periods of time."[203] More specifically, its operational objectives have included stopping Iranian arms transfers to Hezbollah and preventing Iran from entrenching in Syria.[204]

In the interviews for this thesis, the participants explained that cyber operations are unequivocally part of the CBW, although the strategy is not limited to cyberspace and does not treat

[198] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 25.
[199] Goldenberg et al., 'Countering Iran in the Gray Zone: What the United States Should Learn from Israel's Operations in Syria', 8.
[200] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 25.
[201] Eisenkot and Siboni, 'The Campaign Between Wars'.
[202] Dmitry (Dima) Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', *The Washington Quarterly* 40, no. 2 (3 April 2017): 169–70, https://doi.org/10.1080/0163660X.2017.1328928; Eisenkot and Siboni, 'The Campaign Between Wars'.
[203] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 29.
[204] Author interview with Itai Brun.

cyberspace as a distinct strategic domain.[205] Rather, as Gadi Eisenkot, former IDF Chief of Staff, and Gabi Siboni explained, the CBW aims to engage whatever means necessary to counter Iranian threats to national security, regardless of their form, and allow Israel to further develop its own capabilities, thus preparing for the next conflict.[206] At the same time, as one former defence official noted, "cyber is the perfect domain for mabam," because it allows you to conduct offensive action in "a more elegant, stealthy, quiet mode."[207] Cyber tools also allow for the remote execution of attacks to disrupt enemy capabilities (and here the joint United States-Israeli Stuxnet operation, discussed in Chapter 3, comes to mind most prominently, although it took place before CBW was developed as a coherent strategy).[208] What this shows is that in the minds of Israeli security officials, cyber means are regarded as another useful tool to use as part of a wider strategy of demonstrating superiority of force over the adversary in order to, over the medium and long-term, achieve a deterrent effect.

As we already mentioned, the IDF strategy explicitly states that the CBW fits into a broader deterrence objective.[209] According to Adamsky, in keeping with Israeli conventional deterrence thinking, actions within the CBW are not meant to set thresholds per se – instead, the deterrent effect arises from the reputation that Israel accrues through engaging in a continuous limited war under the CBW and through depriving the adversary from acquiring capabilities. In other words, the Israeli deterrence logic foresees convincing the adversary that Israel is prepared to exercise its full military might at any time if provoked and, by coupling this with the degradation of adversary capabilities, it seeks to undermine the confidence of the adversary to such a degree that they "don't even *think* of attacking [Israel] [emphasis added]."[210] Important in this regard is the focus on offensive action and the use of force in the CBW, which comes as no surprise in light of Israel's strategic culture extolling offensive strategy.

In designating the use of force as one of the CBW's primary instruments, the strategy also highlights Israel's high tolerance for risk – a recurring theme in this analysis that distinguishes Israel as the quintessential threat society. According to Eisenkot and Siboni, "Israel's military and political leadership are well aware that this pattern of action involves risks and friction that could spark wider military confrontation or even full-scale war."[211] Indeed, many of the actions under the CBW have involved military strikes (with limited casualties) on Iranian weapons and rocket depots, Iran's

[205] Author interview with former senior defence official; Author interview with Gabi Siboni; Author interview with senior military cyber defence official; Author interview with Daniel Moore.
[206] Eisenkot and Siboni, 'The Campaign Between Wars'.
[207] Author interview with former senior defence official.
[208] Siman-Tov and Even, 'A New Level in the Cyber War between Israel and Iran'.
[209] Israel Defense Forces (transl. Belfer Center for Science and International Affairs), 'Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces', 25.
[210] Adamsky, 'From Israel with Deterrence', 173; Eisenkot and Siboni, 'The Campaign Between Wars'.
[211] Eisenkot and Siboni, 'The Campaign Between Wars'.

command headquarters, and intelligence and logistics sites around Damascus in Syria.[212] Despite the risk of losing planes and pilots at the hands of Syrian or Russian forces, Israel also conducts regular sorties into Syrian airspace using advanced, fixed wing aircraft, preferring this to lower risk, guided, stand-off munitions fired from outside Syria's borders.[213] The air strike on Hamas' cyber headquarters in 2019, as well as being a case of retaliation, was also part of the CBW: a military capability was used to prevent Hamas from engaging in further cyber operations.[214]

Thus, while Israel aims to conduct the CBW under the threshold of what it considers to be war, that threshold is much higher than what other countries would be willing to risk – as evidenced by the use of war planes and cruise missile bombs inside other countries as a matter of routine.[215] This risk acceptance, in keeping with the central argument of this chapter, is primarily a result of the threat society identity. Once again, the siege mentality leads Israel to engage in violent actions to prevent Iran from acquiring more advanced capabilities that could directly threaten Israel's existence. The problem-solving mentality, the preference for "action over reflection,"[216] means that Israeli policymakers do not devote lengthy consideration to potential side effects or unintended consequences, preferring instead to engage in swift action. The cult of the offense, as we discussed above, means that the CBW involves the routine use of force. The threat society, in sum, is the main factor shaping Israel's doctrines, strategies, and operational decisions.

5.5.2 Low-end measures: resilience-building and consequence management

The risk framework in Chapter 3 indicated that, alongside preventive practices, risk societies are likely to be particularly focused on resilience-building and consequence management as a general response to the emergence of cyber conflict – we should also consider here whether Israel engages in such practices. Indeed, although Israel is a threat society, it also seeks to strengthen the resilience of its digital infrastructures and put in place plans for managing the consequences of cyber attacks. Importantly, however, Israeli policymakers do not prioritise resiliency measures in the context of addressing state-sponsored cyber operations. Instead, such measures are mainly meant to protect organisations from lower-end and medium threats such as cyber crime and, in the context of high-end cyber operations, only complement a deterrence strategy.[217]

[212] Goldenberg et al., 'Countering Iran in the Gray Zone: What the United States Should Learn from Israel's Operations in Syria', 8.
[213] Goldenberg et al., 9.
[214] Author interview with former senior defence official.
[215] Author interview with Daniel Moore.
[216] Shapira, 'Israeli National Intelligence Culture and the Response to COVID-19'.
[217] Adamsky, 117–18.

Resilience-building and consequence management appear in the second layer of Israel's Concept of Operations in the National Cyber Strategy, termed there "Systemic Cyber Resilience."[218] The responsibility for these practices falls to the Israeli Computer Emergency Response Team (IL-CERT), which works with organisations affected by a cyber incident to mitigate its effects, prevent malware from spreading further, and aid system recovery.[219] High end threats "by determined, resource-rich attackers who pose a serious danger to the nation," which have been the focus of this chapter, are addressed as part of the third layer of the Concept of Operations, termed "Defense."[220] As Adamsky noted, "[a]lthough Israeli cyber experts dub the third layer 'defense,' it is much more offensive in nature" and "enables deterrence by punishment."[221] At this level, as we already discussed, the focus of policymakers is on the attacker, not the type of attack.[222] Because Israel integrated its signals intelligence unit (the famous Unit 8200) into the military, it is solely the IDF that handles high-end cyber operations (while the responsibility for the two first layers of the Concept of Operations falls mainly to the National Cyber Directorate).[223] As we also discussed earlier, this leaves cyber-related decision-making particularly susceptible to strategic cultural influences, which are disdainful of approaches that prioritise defensive strategies, lauding instead offensive action.

The case of Israel, a threat society, is thus illustrative of the differences between threat societies and risk societies in the context of what Chapter 3 called risk management practices. While in risk societies risk management practices form a central pillar through which states address cyber issues, in Israel they are a compliment to a deterrence-based approach. As such, unlike in countries where preventive actions falls under risk management, in Israel, because the stated objective of the CBW is deterrence, preventive action cannot be viewed as a risk management practice. Risks are usually diverse and potential, while deterrence is constructed against a concrete actor with clear (perceived) intentions and capabilities (a threat).[224]

While Israel does engage in resilience-building and consequence management (albeit under a single heading of Systemic Cyber Resilience), these practices tend not to be included in national security discussions – for example, in the interviews for this project, none of the interviewees mentioned such practices as a means for addressing national-level cyber challenges. Instead, as this chapter has shown, the locus of the conversation is on the place of cyber operations within Israel's broader conflict with Iran and priority is given to deterrence logics.

---

[218] National Cyber Directorate, 'Israel National Cyber Strategy In Brief' (Prime Minister's Office, State of Israel, September 2017), 11, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.
[219] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', 117.
[220] National Cyber Directorate, 'Israel National Cyber Strategy In Brief', 12.
[221] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', 118.
[222] Author interview with Eviatar Matania; Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, 'A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy', *Georgetown Journal of International Affairs* 17, no. 3 (2016): 81, https://doi.org/10.1353/gia.2016.0038.
[223] Author interview with Eviatar Matania.
[224] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London; New York: Routledge, 2010), 18–19.

5.6 Conclusion

This chapter argued that Israel exhibits a pattern of meaningful punishment in response to cyber attacks because it is a threat society, which in turn is a product of three particular elements of Israeli strategic culture. These elements, the siege mentality, the problem-solving attitude, and the cult of the offense, are incompatible with risk avoidance; rather, these features cultivate a firm focus on a single existential threat, increase the willingness to take risks, and predispose a state towards reactivity. Strategic culture in Israel has a particularly strong impact on societal dispositions and political decision-making as a result of compulsory military service, the presence of former military officials in government positions, and a history of political conflict, which leads Israelis to regard the IDF as the guarantor of state survival.[225] The chapter showed that Israel's threat society identity shaped Israeli perceptions of its material threat environment, in particular the Iranian threat, the formulation of the strategy of deterrence, and decision-making on how to respond to cyber aggression.

In terms of structure, after providing an overview of Israel's responses to cyber attacks, the chapter discussed the three features of Israel's strategic culture that create Israel's threat society identity and analysed their influence on Israel's conventional deterrence strategy, which hinges on Israel building and maintaining a reputation for forceful retaliation. It further showed that Israeli policymakers transplanted the same conventional deterrence logic to the cyber domain with a focus on the attacker (as opposed to cyberspace as a distinct strategic domain), the prioritisation of forceful punishment and an acceptance of escalation risks, and the desire to preserve some element of unpredictability in its responses. Honing in on the attacker, the chapter showed that Israeli perceptions of Iran as an existential threat, themselves a product of the siege mentality, shaped Israel's view of cyber conflict as being another "Iran problem." The argument of the chapter was then illustrated in an analysis of Israel's response to Iran's cyber attack on its water infrastructure, demonstrating that Israel's decision-making calculus was in this case characteristic of a threat society.

The final section of the chapter analysed Israeli strategies and actions that, upon first glance, might look like the risk management practices, which Chapter 3 described as being typical of risk societies. The analysis showed that while the Israeli CBW (which in itself is heavily influenced by Israel's threat society identity) includes preventive activities, its explicit deterrence function prevents it from being conceptualised as a risk management practice. The analysis also indicated that although Israel also engages in resilience-building and consequence management, these practices are not typically prioritised by the security community, which holds a strong preference for reactive and offensive strategies.

[225] Handel, 'The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security', 542.

In sum, the chapter showed that Israeli responses to cyber attacks were strongly influenced by ideational factors: Israel's threat society identity, which is in turn a product of strategic culture, determined decisionmakers' perception of Israel's main adversary as an existential threat and shaped security doctrine, leading policymakers to disregard the operational risks of cyberspace and, ultimately, to issue meaningful responses to cyber attacks.

The question that arises is whether Israel's culturally-engrained resolve to punish is translating into an effective cyber deterrence strategy – some might point to the empirical record of continuous low-level conflict between Iran and Israel to suggest that so far it is not.[226] To this question, Israeli policymakers might reply that it is still too early to judge the effectiveness of their deterrence strategy because cyber operations are a relatively new tool of statecraft and establishing a reputation as a tough retaliator takes time. The implication of such a statement is that we are likely to see significant instability for the foreseeable future. There is one final point to consider. As Itai Brun noted, in Israel there is a tendency for strategy formation to follow action, a peculiarity which is again a product of Israelis' problem-solving attitude.[227] It may therefore be the case that Israeli strategists have not yet carefully considered the implications of the strategic environment of cyberspace (particularly its interconnectedness) for strategy. What this chapter makes clear, however, is that even once they do, any new strategy for the cyber domain is likely to be shaped significantly by Israel's threat society identity and thus preserve risk-acceptance at its core.

[226] Work and Harknett, 'Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges', 7.
[227] Author interview with Itai Brun.

Chapter 6
Estonia: A Threat Society Embedded in a Risk Community Alliance

It was all about Russia, always.
General (ret.) Riho Terras, Chief of Staff of the Estonian Defence Forces (2011-2018)[1]

6.1 Introduction

In the spring of 2007, Estonia became the first victim of a major act of international cyber disruption.[2] A series of distributed denial of service (DDoS) attacks, believed by the Estonian authorities to have been sponsored by the Russian state, paralysed online services in the country for weeks. At the time of the attacks, Estonia was already a member of NATO, a membership it had doggedly pursued since regaining independence in 1991 to ensure protection against Russian aggression. At a time when Estonia's tensions with Russia were at the highest since the breakup of the Soviet Union,[3] it chose not to invoke any of the relevant articles of NATO's Washington Treaty to initiate formal alliance proceedings against Russia.

This chapter will argue that Estonia chose not to formally request NATO's help in the case of the 2007 cyberattacks because it yielded to NATO's sensitivities as a "risk community," that is, an alliance dominated by risk societies.[4] As a risk community, NATO paid attention to the operational uncertainties of the cyber domain and was reluctant to respond due to the perceived risk of escalation. As for Estonia, a threat society, officials perceived the existential threat from Russia to be so great that the country decided to accommodate the risk sensitivities of NATO in order to preserve the alliance's commitment in the case of a future, more severe crisis with Russia. In showing the causal importance of beliefs and identities in the interaction between a threat society and a risk community, this chapter will further illustrate the importance of ideational factors in influencing states' perceptions of material reality and shaping responses to foreign cyber attacks.

The chapter will start by describing the 2007 distributed denial of service (DDoS) attacks experienced by Estonia and showcase their relevance to national security. It will argue that, given the

[1] Author interview with Riho Terras, 30 March 2021.
[2] Mils Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', in *Hybrid Threats: A Strategic Communications Perspective Annex of Case Studies*, ed. Benjamin Heap (Riga, Latvia: NATO Stratcom Centre of Excellence, 2019), https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia.
[3] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian*, 17 May 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.
[4] Christopher Coker, *Globalisation and Insecurity in the Twenty-First Century: NATO and the Management of Risk*, Adelphi Papers ; No. 345 (Oxford and New York: Oxford University Press for the International Institute for Strategic Studies, 2002), 66.

severe disruption they caused and the fact that, as the interviews revealed, the Estonians had no doubt as to their sponsorship by the Kremlin, we would expect Estonia to issue a response. To set the context for the explanation of Estonia's lack of response, the chapter will first show that Estonia's threat society identity was a result of the country's historical and ideological perception of Russia as an existential threat and its Finnish-inspired strategic culture emphasising the pursuit of self-reliance[5] and a "fighting spirit." The chapter will then explain that Estonia's threat sensitivity to Russia was so strong that it decided to pursue two defence models simultaneously to ensure full redundancy: the Finnish total defence model *and* collective defence under NATO. Moreover, Estonia's desire for NATO accession and assimilation was equally strong: in order to "fit in" at NATO, Estonia even shaped its official national security policy to align with the NATO risk community's focus on transnational risks. The attainment of NATO membership after years of anxious pursuit was therefore of momentous significance to Estonia; notably, however, further underscoring Estonia's consuming fear of Russia, the country retained military conscription even after joining NATO, unlike many other eastern European countries, and continually feared NATO abandonment.

Having discussed and contextualised Estonia's security thinking in the 2000s, the chapter will then turn to investigating why Estonia did not choose to initiate formal NATO proceedings against Russia in 2007. The analysis will find that the reason for Estonia's decision not to invoke NATO's Article IV (which initiates formal member consultations[6]) was Estonian policymakers' awareness of NATO's risk community nature and their perception of NATO's unwillingness to risk escalating a conflict with Russia (due to the uncertain nature of the cyber domain, particularly with regard to attribution). Concerned about retaining NATO's commitment in the case of a Russian invasion, Estonia chose to refrain from pressuring the alliance to respond. Embedded in a risk community and fully consumed by the Russian existential threat, the Estonian threat society reacted by conforming to the sensitivities of NATO.

The final section of the chapter will examine whether as a result of the attacks, Estonia became more reflexive as a society; it will ask: did the country move up the risk spectrum after 2007? It will argue that, although Estonia *appeared* to become more concerned with risks and seemed to engage in risk management practices after the attacks, it in fact retained its focus on Russia as a primary existential threat and, as a result, did not undergo a shift in identity.

[5] It should be noted here that the pursuit of self-reliance in Estonia's case translates in practice into building up a citizen reserve army to fight a guerrilla war against an invading nation until alliance forces arrive.
[6] NATO, 'The North Atlantic Treaty', 4 April 1949, http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

6.2 The relevance of the 2007 cyber attacks to Estonia's national security

The cyber campaign of 2007 took the form of large scale, coordinated DDoS attacks, which involve websites being flooded and overwhelmed with information requests, thus making them unavailable to legitimate Internet users.[7] The most notable affected websites were those of the Estonian presidency and parliament (*Riigikogu*), almost all of Estonia's government ministries, major political parties, three of the country's largest news organisations, and its two largest banks.[8] The attacks were triggered by the Estonian government's decision to relocate a statue commemorating the Soviet Union's victory over Nazi Germany, the Bronze Soldier, from Tallinn's city centre to a military cemetery on the outskirts of the city. They were accompanied by street rioting and looting by thousands of protesters in Tallinn among the country's Russian ethnic minority, as well as a breach of the Estonian embassy compound in Moscow by "Nashi" political activists tied to Vladimir Putin's political party.[9] The cyber attacks were particularly destabilising due to Estonia's extreme dependence on digital technologies. In the month preceding the start of the attacks, Estonia held the world's first-ever general election using Internet voting.[10] Already at the time, 95-97% of banking transactions in the country were performed online.[11]

The attacks began on April 26th, 2007, the first day of the excavation works around the Bronze Soldier. They came in multiple waves. The most sophisticated and coordinated wave lasted from May 4th to May 9th (Russian victory day) and targeted Estonia's major banks, producing severe disruption to citizens' daily lives.[12] The network of computers used in the attacks spanned 175 national jurisdictions and included between one and two million machines or "bots."[13] The financial and intellectual resources required to execute such precisely timed attacks indicated that these had a central command and control – they were not the work of ordinary people.[14] Toomas Hendrik Ilves, Estonia's President at the time, recounted that when he visited the Estonian Computer Emergency Response Team (CERT) on May 9th, the DDoS attacks started at 00:00:00 GMT and rose to an "amazing level," before shutting off

[7] Will Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 110.
[8] Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'.
[9] Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', 56; The Economist, 'A Cyber-Riot', *The Economist*, 10 May 2007, https://www.economist.com/europe/2007/05/10/a-cyber-riot.
[10] 'I-Voting', e-Estonia, accessed 4 March 2019, https://e-estonia.com/solutions/e-governance/i-voting/.
[11] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010), 17, 22.
[12] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 110; Lucas Kello, 'The Advantages of Latitude: Estonia's Post-Communist Success Story', in *Democratization and Security in Central and Eastern Europe and the Post-Soviet States*, ed. David Bosold, Petr Drulák, and Nik Hynek (Baden-Baden: Nomos, 2012), 50; Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', 53.
[13] Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', 53.
[14] Tikk, Kaska, and Vihul, *International Cyber Incidents*, 23.

abruptly at exactly 23:59:59 GMT."[15] The entire campaign was terminated, again in a highly coordinated fashion, on May 19th.[16]

While the attacks were still taking place, on May 1st, Estonia's Foreign Minister, Urmas Paet, issued the following statement: "Russia is attacking Estonia … IP [Internet Protocol] addresses have helped to identify that the cyber terrorists' attacks against the Internet pages of Estonian government agencies and the Office of the President have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation."[17] Russian officials, however, denied the allegations and suggested that professional hackers, empowered by the ease of access to offensive cyber tools, could have feasibly hijacked the IP addresses of Russian officials to make the operations appear to be state-sponsored.[18] Despite the existence of significant circumstantial evidence pointing to Russian government involvement, Jaak Aaviksoo, Estonia's Defence Minister, crawled back the Foreign Minister's attribution statement. "[A]t the moment, I cannot state for certain that the cyber attacks were managed by the Kremlin, or other Russian government agencies," he said.[19]

The focus on Russia narrowed substantially after Moscow did not respond to an official Estonian request in June 2007 for assistance in the attacks' investigation, despite the existence of a bilateral Mutual Legal Assistance treaty between the two countries, which specifically stipulated this kind of cooperation.[20] Indeed, explained Lauri Almann, the Permanent Undersecretary of the Ministry of Defence at the time, out of many jurisdictions through which the attacks were routed, "you see one that did not want to cooperate with us and it was Russia. So their silence spoke volumes."[21] The Russian response to the request cited procedural problems as a barrier to cooperation with the Estonian State Prosecutor.[22] More likely, Russia refused to cooperate knowing that further investigations into the

---

[15] Author interview with Toomas Hendrik Ilves, 25 March 2021.
[16] Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', 55.
[17] Government of the Republic of Estonia, 'Declaration of the Minister of Foreign Affairs of the Republic of Estonia', Government Office, 1 May 2007, https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia.
[18] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 113.
[19] Aaviksoo quoted in: TBT staff and wire reports, 'Police Conclude Probe into Alleged Riot Ringleaders', The Baltic Times, 6 September 2007, https://www.baltictimes.com/news/articles/18742/.
[20] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 110; Rain Ottis, 'Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective', in *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth* (Reading: Academic Publishing Limited, 2008), 3, https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.
[21] Lauri Almann speaking in: Center for Strategic & International Studies (CSIS), *10 Years of Cyber Estonia: What Will the Next Decade Bring?* (Washington, D.C.: Center for Strategic & International Studies, 2017), https://www.csis.org/events/10-years-cyber-estonia-what-will-next-decade-bring.
[22] Sico van der Meer, 'Foreign Policy Responses to International Cyber-Attacks', Policy Brief (Clingendael Netherlands Institute of International Relations, September 2015), 3, https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf.

incident would unequivocally reveal the involvement of the Russian state in the attacks.[23] Accompanying the cyber attacks and street riots were also Russian actions to disrupt Estonian trade, including a Russian boycott of Estonian goods and the creation of intentional obstacles to rail and truck traffic at the Estonian-Russian border.[24]

On the technical front, the cyber attacks were traced to a botnet associated with a Russian cybercrime group operating from St Petersburg with links to the so-called Russian Business Network.[25] "Patriotic hackers" were also recruited on online Russian language forums where instructions, tools and target lists were posted, enabling the individuals to volunteer their personal computers to the botnet attacking Estonian web servers.[26] The operations were further traced to the Nashi activist group.[27] Mainly, however, it was a case of well-resourced actors renting a botnet to overwhelm particular servers – hence why the attacks ceased abruptly once the rented time had been exhausted. "It was a unique public-private partnership between the Kremlin and the mafia," affirmed Ilves.[28]

As the attacks unfolded, Estonian decision-makers debated the implications of the attacks for collective defence in the context of the NATO alliance.[29] Ene Ergma, President of the Estonian Parliament at the time, highlighting the relevance of the attacks to NATO, said on August 21st: "Estonia is a NATO country. Attacking us is one way of checking NATO's defenses. They could examine the alliance's readiness under the cover of the statue protest."[30]

Eventually, only a single individual, Dmitri Galushkevich, an ethnic Russian student, faced criminal charges in Estonia for targeting a political party's website from within the country's borders.[31]

---

[23] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 114.
[24] U.S. Embassy in Estonia, 'Russian Bear Hug Squeezes Estonian Economy', Wikileaks Public Library of US Diplomacy (Tallinn, Estonia: U.S. Embassy in Estonia, 29 May 2007), https://wikileaks.org/plusd/cables/07TALLINN347_a.html.
[25] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman & Littlefield, 2017), 43.
[26] Scott Applegate, 'Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare', *Security & Privacy, IEEE* 9, no. 5 (2011): 17, https://doi.org/10.1109/MSP.2011.46; Jasper, *Strategic Cyber Deterrence*, 44.
[27] Michael N. Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', *Fletcher Security Review* 1, no. 2 (2014): 56; James Jones, 'Putin's Youth Movement Provides a Sinister Backdrop to Russia's Protests | James Jones', *The Guardian*, 8 December 2011, sec. Opinion, https://www.theguardian.com/commentisfree/2011/dec/08/putin-russia-elections.
[28] Author interview with Toomas Hendrik Ilves.
[29] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 186.
[30] Ergma cited in: Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', *Wired*, 21 August 2007, https://www.wired.com/2007/08/ff-estonia/.
[31] van der Meer, 'Foreign Policy Responses to International Cyber-Attacks', 3; Hills, 'Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia', 61. In 2009, a Russian State Duma Deputy, Sergei Markov, announced that his assistant, Konstantin Goloskokov, had carried out the cyber operations against Estonia. Goloskokov went on to state that he had conducted the operations on his own, without government support, and as "an act of civil disobedience." The description of the methods Goloskokov claimed to have used, however, only matched part of the attack campaign, the extensiveness of which indicated the involvement of many more individuals with access to significant financial and other resources. See: Applegate, 'Cybermilitias and Political Hackers', 17 and Tikk, Kaska, and Vihul, *International Cyber Incidents*, 24.

Importantly, other than adding individual hackers to the Schengen Black List,[32] there was no clear external response by the Estonian government to the attacks. As we discussed, even a statement from the Foreign Minister that the attacks had originated from the Kremlin was contravened by the Defence Minister.[33] Importantly, Estonia did have response options. It could have, for instance, invoked NATO's Article IV, which provides for member consultations whenever "the territorial integrity, political independence or security of any of the Parties is threatened."[34] The article has been invoked a small number of times in the past, including by Poland in 2014 in response to Russian activities in Ukraine.[35] The result of such consultations is usually a statement of NATO solidarity with the aggrieved country, which, especially in the case of Estonia – still in 2007 a new member of the alliance – would have sent a strong message of resolve to Moscow that aggression towards NATO countries bordering Russia would not be tolerated.

Estonia's international non-response to the cyber attacks seems surprising in light of the fact that the attacks were seen by decision-makers as a national security incident. Aaviksoo called the attacks "a national security situation," which can "effectively be compared to when your ports are shut to the sea."[36] Marina Kaljurand, Estonian Ambassador to Russia at the time, saw the attacks as particularly "disruptive and disturbing to a state that was known for its unique online services."[37]

Indeed, ATM machines and online banking services of the two largest Estonian banks were disrupted for a period of three weeks with significant implications for the domestic economy, which was almost entirely reliant on electronic transactions.[38] Hansabank, Estonia's biggest bank, sustained losses in revenue of 10 million euros.[39] In an effort to keep the banks' websites available for domestic users, Estonia's CERT reacted to the attacks by halting foreign internet traffic, with significant financial implications for the banks' foreign business.[40]

---

[32] Michael Miklaucic, 'An Interview with Marina Kaljurand, Former Minister of Foreign Affairs of Estonia', *PRISM* 7, no. 2 (2017): 116.
[33] Adrian Blomfield, 'Russia Accused over Estonian "Cyber-Terrorism"', *The Telegraph*, 17 May 2007, https://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html.
[34] NATO, 'The North Atlantic Treaty'.
[35] NATO, 'Statement by the North Atlantic Council Following Meeting under Article 4 of the Washington Treaty', 4 March 2014, http://www.nato.int/cps/en/natohq/news_107716.htm.
[36] Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia', *The New York Times*, 29 May 2007, sec. Technology, https://www.nytimes.com/2007/05/29/technology/29estonia.html.
[37] Marina Kaljurand featured in: Bertelsmann Foundation, 'Episode 1 Russian Cyber-Attack on Estonia', Bertelsmann Foundation, 4 February 2021, https://bfna.org/politics-society/episode-1-russian-cyber-attack-on-estonia/.
[38] Tikk, Kaska, and Vihul, *International Cyber Incidents*, 17, 22.
[39] U.S. Embassy in Estonia, 'Russian Bear Hug Squeezes Estonian Economy'.
[40] van der Meer, 'Foreign Policy Responses to International Cyber-Attacks', 2; The Economist, 'A Cyber-Riot'; Ottis, 'Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective', 2; Tikk, Kaska, and Vihul, *International Cyber Incidents*, 22; Peeter Lorents, Rain Ottis, and Raul Rikk, 'Cyber Society and Cooperative Cyber Defence', in *Internationalization, Design and Global Development*, ed. Nuray Aykin, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2009), 184, https://doi.org/10.1007/978-3-642-02767-3_20.

The Estonian government also had to increase Estonia's broadband capacity eightfold in order for it to remain operational – an extremely expensive move.[41] On top of this, government employees were not able to use email, the government's online media briefing room was unavailable, and the websites of three of Estonia's six largest media outlets were disrupted, resulting in what was effectively a "partial information blockade."[42] Because the attacks also targeted the servers of three major Internet Service Providers (ISPs), many small and medium sized enterprises were unable to conduct their daily business, forcing Estonia to block all Internet traffic from abroad for a period of time.[43] Finally, and perhaps most damagingly, the attacks had a social and psychological effect on Estonian domestic publics. At the time of the attacks, Aaviksoo stipulated that their objective was to "destabilise Estonian society" and create widespread anxiety and undermine trust in digital services in a country completely dependent on their functioning – a type of "psychological terror."[44] There is therefore little doubt that, from the perspective of the Estonian political leadership, the attacks amounted to an issue of national security.

Finally, there is the attribution question, which was not as complicated, technically or politically, as Aaviksoo had indicated in his public remarks at the time.[45] A leaked US diplomatic cable from May 29th 2007 stated that, "the political nature of the attacks clearly suggests coordinated Russian involvement."[46] In an interview for this research, Aaviksoo himself affirmed, "if it looks like a dog, barks and bites like a dog, then most probably it is a dog," suggesting that the attacks bore the hallmarks of Russian state action.[47] According to Merle Maigre, then Deputy Head of NATO's Liaison Office in Kiev and later President Ilves' Security Policy Adviser, "there was no doubt that the Russian government was involved in and was behind these attacks."[48] Leaked cables detailing conversations between Estonian officials and the US embassy in Tallinn around the time of the attacks also reveal that the Estonian government believed Russia was behind the campaign.[49] Even if Estonia lacked "smoking gun" evidence and was not comfortable with attributing the operation on the basis of available technical

[41] U.S. Embassy in Estonia, 'Russian Bear Hug Squeezes Estonian Economy'.
[42] Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News*, 27 April 2017, https://www.bbc.com/news/39655415; Lorents, Ottis, and Rikk, 'Cyber Society and Cooperative Cyber Defence', 184.
[43] Tikk, Kaska, and Vihul, *International Cyber Incidents*, 24; Council on Foreign Relations, 'Estonian Denial of Service Incident', Council on Foreign Relations, May 2007, https://www.cfr.org/cyber-operations/estonian-denial-service-incident.
[44] Aaviksoo quoted in: Piret Pernik et al., 'The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine' (European Union Institute for Security Studies (EUISS), 2018), https://www.jstor.org/stable/resrep21140.9.
[45] Aaviksoo quoted in: TBT staff and wire reports, 'Police Conclude Probe into Alleged Riot Ringleaders'.
[46] U.S. Embassy in Estonia, 'Russian Bear Hug Squeezes Estonian Economy'.
[47] Author interview with Jaak Aaviksoo, 23 March 2021.
[48] Author interview with Merle Maigre, 19 March 2021.
[49] U.S. Embassy in Estonia, 'Estonia: GOE Officials on the Bronze Soldier, Russia and Integration', Wikileaks Public Library of US Diplomacy (Tallinn, Estonia: U.S. Embassy in Estonia, 11 May 2007), https://wikileaks.org/plusd/cables/07TALLINN310_a.html.

reports, Russia's refusal of legal assistance, with no plausible explanation and in spite of the existence of treaty obligations to help, would have given Estonia sufficient grounds to assign responsibility for the attacks to Putin's government.[50] There is also reason to believe that Estonian policymakers were in favour of a stronger stance and did not see the attribution issue as a significant obstacle. "For every denial of Russia, we should have come back and said 'why can't you [assist our enquiries]?' … [to] elevate the discussion and escalate it more and more," lamented Almann. "The bottom line is, there is one jurisdiction who didn't want to cooperate and there you have your attribution," he reiterated.[51] NATO seemed to be similarly aware of Russian culpability. As one NATO official stated at the time of the attacks: "I won't point fingers. But these [attacks] were not things done by a few individuals. This clearly bore the hallmarks of something concerted,"[52] adding that the attacks were "a serious issue for the alliance as a whole."[53]

Given that the attacks reached the threshold of national security and were understood to have been sponsored by the Russian state, Estonia's decision not to invoke any of NATO's articles to respond to them is puzzling.

6.3 Estonia: a threat society within a larger risk community

First, to grasp the sources of Estonia's nature as a threat society, this section will review the country's historically and culturally shaped perception of Russia as an existential threat and the influence of Finnish strategic culture, especially the "fighting spirit" and a sense of self-reliance, following the country's return to independence in 1991. Second, the section will show that the intensity of Estonia's preoccupation with Russia was so great that the country pursued a unique dual approach of total defence and collective defence. It will discuss the immense importance that Estonia attached to NATO accession, its continuing sense of existential dread vis-à-vis Russia even after joining the alliance, and its related fear of NATO abandonment. Indeed, once Estonia had joined the alliance, demonstrating the intensity of its threat society identity, the country distinguished itself from other NATO allies in retaining conscription within a collective defence structure. Third, the section will investigate why Estonia's 2004 National Security Concept seemed to signify a stark departure from a focus on a single existential threat to concerns characteristic of risk societies. It will argue that Estonia's emphasis on risks in the strategy was paradoxically also a product of its threat society identity: the country superficially aligned its official national security doctrine with NATO's to further its objective of joining the alliance, which it regarded as essential to its own survival.

---

[50] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 114.
[51] Almann speaking at: Center for Strategic & International Studies (CSIS), *10 Years of Cyber Estonia*.
[52] NATO official quoted in: Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'.
[53] NATO official quoted in: Traynor.

6.3.1 Estonia as a threat society

Estonia's identity as a threat society is most visible in its unwavering preoccupation with Russia as a survival threat, even, as we will see, at a time in the 1990s and the early 2000s when western countries were starting to treat Russia as a potential security partner. Fuelling the fear of Russia was Estonia's historical sense of victimhood, an important element of Estonian national identity born from the national trauma of the almost 50-year Soviet occupation, which saw political murders, mass deportations, forced russification and widespread oppression.[54] The characteristic threat society fixation with a single, well-defined adversary was in fact so great that upon regaining independence in 1991, Estonia decided to adopt Finland's model of "total defence," which prioritised compulsory military service, large reserve armies, and preparation for sustained guerrilla warfare in case of invasion.[55]

In addition to sharing ethnic, cultural, and linguistic affinities with Finland, Estonia's leaders greatly admired the country for the way it had fought Russia in the Winter War of 1939-40, when, despite sustaining territorial losses, Finland retained its independence – unlike Estonia, which in 1940, under intense pressure from Moscow, had agreed to allow the stationing of Soviet troops in its territory rather than immediately fighting them.[56] Estonian diplomat Margus Kolga even described Estonia as bearing strong "emotional feelings" in relation to the Finnish Winter War.[57] Finnish military culture, which prioritised a fighting spirit, courage, grit, and the pursuit of self-reliance (*sisu*), was therefore regarded in Estonia as a model to be emulated.[58] What significantly aided the total defence model's diffusion into Estonian strategic thinking was Estonia's decision to train its non-commissioned officers and officer corps in Finland before the country established its own military academy in 1998.[59]

The admiration for Finland's defence culture dovetailed with Estonia's resolve to never experience a repeat of 1940 – and this is how a characteristic threat society sense of self-reliance and determination to "fight back" against the enemy was born. Thus, for example, particularly popular in the 1990s in Estonia was the narrative of the so-called "Forest Brothers," which described how under Soviet occupation Estonian "soldiers" fought Soviet troops and agents in Estonia's forests as part of "the nation's long-lasting struggle for independence."[60] Illustrating the strength of beliefs from strategic

[54] Kaarel Piirimäe, 'From an "Army of Historians" to an "Army of Professionals": History and the Strategic Culture in Estonia', *Scandinavian Journal of Military Studies* 3, no. 1 (2020): 102, 105, https://doi.org/10.31374/sjms.37.
[55] Holger Mölder, 'The Development of Military Cultures', in *Membership: Twenty Years of Defence Development in the Baltic States*, ed. Tony Lawrence and Tomas Jermalavičius (Tallinn, Estonia: International Centre for Defence Studies, 2013), 91.
[56] Mölder, 105.
[57] Kolga quoted in: Mölder, 105.
[58] Mölder, 105.
[59] Republic of Estonia Defence Forces, 'Military Education', 27 February 2020, https://mil.ee/en/defence-forces/military-education/.
[60] Piirimäe, 'From an "Army of Historians" to an "Army of Professionals"', 105.

culture, what this popular version neglected to mention was that many of these people were in fact unarmed and merely hiding in the forests from Soviet authorities.[61]

Over the years, Estonia continued to demonstrate its characteristic threat society preoccupation with menacing Russian behaviour. It also showed a tendency towards reactivity in its tough rhetoric against Russia, for example in the following statements: In 2008, commenting after Russia's invasion of Georgia, Ilves explained, "[i]f you're a country of about 1.3 million, and you're being bullied by a country of 142 million, someone's got to stand up and say something."[62] Riho Terras, Chief of Staff of the Estonian Defence Forces, reasoned after the Ukraine crisis that if Russian forces or "little green men" were to enter Estonia, "you should shoot the first one to appear."[63] Eerik-Niiles Kross, Estonia's former Chief of Intelligence Services, castigated the west for its weak response to Russian aggression:

> There was not even a good set of threats. Obama, of course, always said the military option is off the table. … A strong Western response would have been this: The moment the first little Green Men arrived, the phone call to Putin, 'Ok, Volodya, you have 24 hours to get the [expletive] out of there, my Sixth Fleet is on the way. … Putin's not reading the speeches. … He's reading the signs, and what is the action? He's like a blatnoi [thug] in a prison cell. He wants to see this new guy, with food from home in his bag, can I take it from him or not? That's his thing.[64]

Estonian policymakers demonstrated a particular attachment to the strategy of deterrence by punishment – which is again characteristic of a threat society. Defence Minister Sven Mikser explained that, "when dealing with any sort of regime like that of Mr Putin's, weakness is more provocative than strength. It is very important that the West is … strong and united. That is the best way to deter Russia."[65] Showcasing similar deterrence thinking and the pursuit of self-reliance, Aaviksoo underscored the necessity of maintaining self-sufficiency through the possession of an arsenal of capabilities and convincing the adversary through "demonstrations of self-assertion" of your "readiness to use them, including in the so-called 'final fight'." He further advocated, in true threat society fashion, for "taking risks if necessary with death" because "freedom [is] the ultimate and uncompromising value."[66] Threat society reactivity was also noticeable in the immediate reaction to the 2007 cyber attacks: recall that the Estonian Foreign Minister Urmas Paet publicly and vehemently accused the

---

[61] Piirimäe, 105.
[62] Gregory Feifer, 'Estonia Seeks Stronger EU Response To Russia', NPR.org, 9 September 2008, https://www.npr.org/templates/story/story.php?storyId=94428390.
[63] Sam Jones, 'Estonia Ready to Deal with Russia's "Little Green Men"', *Financial Times*, 13 May 2015, https://www.ft.com/content/03c5ebde-f95a-11e4-ae65-00144feab7de.
[64] Politico, 'Eerik-Niiles Kross: The Baltic James Bond', *Politico*, 7 December 2017, https://www.politico.eu/list/politico-28-2018-ranking/eerik-niiles-kross/.
[65] David Mardiste, 'Show Putin Strength, Not Weakness, Says Estonian Defense Minister', *Atlantic Council* (blog), 10 November 2014, https://www.atlanticcouncil.org/blogs/natosource/show-putin-strength-not-weakness-says-estonian-defense-minister/.
[66] Jaak Aaviksoo, 'Meie Olemine Ja Kestmine', in *Valik Riigikaitsealaseid Artikleid II* (Tallinn, Estonia: Kaitseministeerium, 2008), 3.

Kremlin of perpetrating the attacks.[67] The statement was then reined in by Aaviksoo, probably, as we will see in later sections, as a result of the awareness of sensitivities at NATO.

It is not difficult to see how the strategic culture of total defence that Estonia adopted from Finland, focusing on the fighting spirit and pursuit of self-reliance, combined with historical memory of Soviet trauma to produce a threat society identity in Estonia after 1991. As we will see in the next section, this threat society identity was preserved even after Estonia joined NATO – Estonia did not believe that collective defence would be enough to ensure its security from the Russian threat.

6.3.2 In search of NATO: combining total defence with collective defence

Estonia's historical perception of Russia as an existential threat is crucial for understanding the immense importance that Estonia attached to joining NATO, regarded by Estonian officials and the general public as an "existential necessity,"[68] and its retainment of total defence under the umbrella of the alliance. According to surveys conducted by Saar Poll from 2009 to 2012, over 60% of respondents believed that membership in NATO was the most important security guarantee for Estonia.[69] The country's National Security Concepts year upon year emphasised the same view.[70] As we will see later in the chapter, Estonia's almost obsessive preoccupation with gaining and retaining the security guarantee of NATO allies played a pivotal role in its non-response to the 2007 attacks.

According to Jüri Luik, who led the Estonian delegation in negotiations to join NATO, Estonia's road to NATO membership was "complex and controversial"; it was by no means pre-ordained to occur.[71] The most difficult requirements for Estonia to fulfil were the absence of tensions with its neighbour and the resolution of border issues.[72] As Aaviksoo explained, "back in those days NATO was not willing to have new members who were hostile towards Russia."[73]

---

[67] Government of the Republic of Estonia, 'Declaration of the Minister of Foreign Affairs of the Republic of Estonia'.
[68] Michael Weiss, 'The Hero Who Betrayed His Country', *The Atlantic*, 26 June 2019, https://www.theatlantic.com/international/archive/2019/06/estonia-russia-deniss-metsavas-spy/592417/.
[69] Saar Poll, 'Public Opinion and National Defence, March 2012' (Tallinn: Saar Poll, 2012), https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2012_march.pdf.
[70] Ministry of Defence of the Republic of Estonia, 'National Security Concept of the Republic of Estonia (2004)', 2004, 9, https://www.files.ethz.ch/isn/156841/Estonia-2004.pdf; Ministry of Defence of the Republic of Estonia, 'National Security Concept of the Republic of Estonia (2010)', 2010, 4, https://www.kaitseministeerium.ee//sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf; Ministry of Defence of the Republic of Estonia, 'National Security Concept of the Republic of Estonia (2017)', 2017, 12, https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.
[71] Luik.
[72] Luik.
[73] Author interview with Jaak Aaviksoo, 23 March 2021.

The fact that Estonia was eventually able to join NATO was a result of the western rapprochement with Russia at the time: Vladimir Putin, still relatively new in office, had not yet clashed with western interests and, after the attacks of September 11, 2001, had even expressed solidarity with the United States in the global mission to defeat terrorism.[74] As a result, President George W. Bush had come down with what Luik described as the "occupational disease of all newly elected US presidents" in believing that it was possible to negotiate with the Kremlin, thus demoting concerns about enlarging NATO to encompass Russia's "near abroad."[75] Already at this point, we can detect the clash of Estonian and NATO ideas about Russia, which would later have profound repercussions for Estonian decision-making.

As we discussed, becoming a member of NATO by no means erased Estonia's worries about the existential threat it felt from its large eastern neighbour. Two years after joining NATO, the 2006 Annual Review of the Estonian Internal Security Service (KaPo), an organisation famous within the west for its efficiency in exposing Russian spies,[76] pointed to Russian operations as the intelligence community's main national security concern. The sizeable Russian minority living in Estonia (25% of the population, about a third of which hold Russian citizenship and another third of which hold "stateless" passports) was seen as the main conduit for Russian interference in Estonian domestic affairs.[77]

While other western countries were focused on the mission of Russian democratisation, the KaPo singled out Russian "information war," economic pressures, espionage efforts, and incitement of domestic violence as threats to Estonian security.[78] The rioting behaviour of the Russian community in Estonia, according to the KaPo, was "directed and supported directly" by the Russian government and was part of Putin's aggressive foreign policy towards the Baltic States, which was in turn driven by a deeper objective to generate greater Russian influence across the world.[79]

While the KaPo reports also paid some attention to diffused risks such as transnational terrorism, a topic which was dominating security conversations in the United States and western

[74] Michael McFaul, 'Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy', *International Security* 45, no. 2 (1 October 2020): 110, https://doi.org/10.1162/isec_a_00390.
[75] Luik, 'Estonia's Long Road to NATO'.
[76] Weiss, 'The Hero Who Betrayed His Country'.
[77] Kaitsepolitseiamet, 'Security Police of the Republic of Estonia Annual Review 2007' (Kaitsepolitseiamet, 2007), 8–13, https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202007.pdf; Toivo U. Raun, 'Estonia after 1991: Identity and Integration', *East European Politics and Societies* 23, no. 4 (1 November 2009): 527–28, https://doi.org/10.1177/0888325409342113.
[78] The 2007 KaPo report, compiled just after the riots and cyber attacks, stated that "[t]he greatest threat to the state's security … was mass riots in Tallinn and [the eastern region of] Ida-Virumaa, provoked from Russia and followed by cyber attacks [*sic*]." The events surrounding the removal of the Bronze Soldier happened under the "threatening shadow of hostile Russia." See: Kaitsepolitseiamet, 'Security Police of the Republic of Estonia Annual Review 2007', 8–17.
[79] Kaitsepolitseiamet, 12–13.

Europe, the organisation was firmly transfixed on Russia.[80] These sensitivities were consistent with the tone and substance of Putin's infamous speech at the Munich Conference in 2007, where he cautioned that NATO expansion to Russia "represents a serious provocation."[81] Despite Putin's clear exposition of an oppositional vision of relations between Russia and the west, the interviews with former Estonian officials for this project revealed that they believed western countries did not truly "wake up" to the threat of Russia until Russia's annexation of Crimea in 2014.[82]

Leaked diplomatic cables from the late 2000s further show Estonians' belief that Russian hostility was particularly intense in relation to Estonia. "Estonian-Russian relations are decided by Putin, not the Kremlin or the MFA [Ministry of Foreign Affairs]," explained Harri Tiido, Estonia's NATO Ambassador at the time of the attacks, "and Putin has a personal gripe with Estonia," possibly because Estonians handed over Putin's father (a Soviet parachutist) to Nazi authorities during World War Two.[83] Similarly, in a meeting with the US Secretary of State, Urmas Paet opined that Russia has a "Cold War mentality" and was staging large military exercises near the borders of Estonia and the other Baltic states to cut them off from the west.[84]

Importantly, these strong worries about the Russian existential threat meant that from the beginning of its membership of NATO, Estonia harboured fears of NATO abandonment.[85] Indications of this fear abounded. One of Estonia's National Security Concepts plainly stated: "the possibility of military attack on Estonia cannot be ruled out if NATO's collective deterrence is not credible."[86] On the eve of a 2008 visit of US Assistant Secretary of State Daniel Fried to Tallinn, the US Embassy there wrote to Fried explaining that the Estonian government was keen to receive assurances from the United States that "Estonia will not be left to its own defences should Russia take aggressive military action against them" and that "Article V of the Washington Treaty is fully in force."[87] As we will see, these fears of NATO abandonment played a particularly important role in Estonia deciding not to pressure

---

[80] Kaitsepolitseiamet, 'Security Police of the Republic of Estonia Annual Review 2006' (Kaitsepolitseiamet, 2006), 2, https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202006.pdf.
[81] The Washington Post (courtesy of the Munich Conference on Security Policy), 'Transcript: Putin's Prepared Remarks at 43rd Munich Conference on Security Policy', The Washington Post, 12 February 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200555.html.
[82] Author interview with Harri Tiido, 30 March 2021; Author interview with Toomas Hendrik Ilves; Author interview with Riho Terras.
[83] Tiido quoted in: U.S. Embassy in Estonia, 'Estonia: Das Quanrud Discusses Afghanistan, Russia, the Economy', Wikileaks Public Library of US Diplomacy (Tallinn, Estonia: U.S. Embassy in Estonia, 16 December 2009), https://wikileaks.org/plusd/cables/09TALLINN371_a.html.
[84] Paet quoted in: 'Secretary Clinton's Meeting with Estonian Foreign Minister Urmas Paet, September 17, 2009, 2:15 P.M., Washington, D.C.', Wikileaks Public Library of US Diplomacy (Washington, D.C: Office of the Secretary of State, 24 September 2009), https://wikileaks.org/plusd/cables/09STATE99089_a.html.
[85] U.S. Embassy in Estonia, 'Scenesetter for A/S Fried's Visit to Estonia', Wikileaks Public Library of US Diplomacy (Tallinn, Estonia: U.S. Embassy in Estonia, 25 September 2008), https://wikileaks.org/plusd/cables/08TALLINN338_a.html.
[86] Ministry of Defence of the Republic of Estonia, 'National Security Concept of the Republic of Estonia (2017)'; Ministry of Defence, 'National Security Concept of the Republic of Estonia (2010)'; Ministry of Defence, 'National Security Concept of the Republic of Estonia (2004)'.
[87] U.S. Embassy in Estonia, 'Scenesetter for A/S Fried's Visit to Estonia'.

the alliance for a response in 2007. Moreover, in the hope of garnering the favour of NATO allies, Estonia sought to make itself as valuable to the alliance as possible and, as section 6.4 will discuss, much of the country's enthusiasm in assuming a later leadership role on European cyber issues was precisely an attempt to carve out an indispensable role within NATO in order to ensure its own security in the event of an Article V scenario.[88]

While seeking collective defence through NATO might seem contradictory to the characteristic threat society pursuit of self-reliance under total defence, what is in fact the case is that, in Estonia's reasoning, the two were meant to complement each other: Estonia sought to create full redundancy in the case of a Russian invasion. Indeed, the fear of NATO abandonment meant that Estonia pursued a unique two-pronged strategy of total defence within a collective defence structure. In particular, Estonia did not move away from the Finnish defence model and maintained compulsory military service even after joining NATO, an approach which enjoyed the support of 90% of Estonia's population.[89] Importantly, it is clear that this stance was not mainly a result of geopolitical factors: Latvia and Lithuania, Estonia's two southern neighbours, share the same external pressures from Russia, but both abolished conscription after joining NATO.[90] Instead, the retention of total defence within a collective defence structure shows us the intensity of the Estonian threat society. So concerned was Estonia about the external Russian threat even after NATO accession, that Estonian leaders believed it was necessary to continue to train a large reserve force even under the umbrella of the Article V guarantee. This stance produced a unique fusion of self-reliance and collective defence, distinguishing the Estonian threat society's defence posture from other NATO countries.

Having already established the cultural and historical roots of Estonia's threat society posture and shown the level of its intensity even after joining NATO, there remains one point that needs to be investigated before discussing Estonia's response to the 2007 attacks – Estonia's seeming articulation of risk society concerns in official policy around the time of the cyber attacks.

6.3.3 Estonia: a risk pretender?

Estonia's 2004 National Security Concept, which was still the governing strategy at the time of the 2007 attacks, placed a striking emphasis on a series of new, unforeseeable, and uncontrollable challenges and risks originating far from Estonia's borders. Here there seems to be a distinct tension between Estonia's strategic culture favouring a fighting spirit and its view of Russia as an existential security threat, on the one hand, and the official defence doctrine focusing on risk, on the other. How, then, did Estonia square its persistent concern with a state-based threat with an increased policy focus

[88] Josh Gold, 'How Estonia Uses Cybersecurity to Strengthen Its Position in NATO', ICDS, 27 May 2019, https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/.
[89] Saar Poll, 'Public Opinion and National Defence, March 2012'.
[90] Mölder, 'The Development of Military Cultures', 114–15.

on transnational risks? This section will explore how Estonia's official defence doctrine was adjusted to align with NATO's security priorities – even as Estonia itself retained its threat society focus on Russia as an existential challenge.

The 2004 Concept was indeed an apparent exemplar of risk society thinking, highlighting the challenges posed by diverse, transnational risks in a new security environment:

> Changes in the international security environment have brought with them new security threats. The unconventional threats among them are: international terrorism; the uncontrolled spread of weapons of mass destruction; organised crime; the smuggling of weapons, narcotics, and people; and the flow of refugees created by crisis situations. In such conditions, no nation or region of the world is beyond danger. For Estonia also, many previously non-important threats have become actual.[91]

The Concept further highlighted that "[t]he *most serious* threats to Estonia's security are possible *instability* and *uncontrollable developments* in the world [emphasis added]." Recall from Chapter 2 that the fear of uncertainty and lack of control are characteristic of risk societies. With reference to the apparent unpredictability of Estonia's new security situation, the Concept added: "[t]he increased probability that new *many-faceted* and often *unforeseeable threats* will crop up presents the ensuring of security with new challenges [emphasis added]."[92] Introducing the new strategy, Margus Hanson, Estonia's Minister of Defence in 2004, explained that "[m]ore than before, Estonia's national security is also being affected by security developments in geographically distant regions."[93] Such an assessment is also indicative of the security logics that Beck identified under the risk society: globalisation, Beck wrote, has led to a "*de-bounding* of uncontrollable risks." Physical distance and nation state boundaries, Beck observed, no longer offered protection from dangers.[94] Indeed, Hanson himself referred to increased global interconnectedness as the source of the new risks: "together with the positive effects of globalisation, the threats associated with it have also become apparent."[95]

Given our discussion in the previous sections about the intensity of the Estonian threat society in the face of the perceived existential threat from Russia, the omission of Russia as a major threat to national security in the Concept is striking. In fact, however, this omission was fully calculated: the timing of Estonia's increased emphasis in public documents on risks coincided with NATO integration

---

[91] Ministry of Defence of the Republic of Estonia, 'National Security Concept of the Republic of Estonia (2004)', 5.
[92] Ministry of Defence of the Republic of Estonia, 5–6.
[93] Ministry of Foreign Affairs of the Republic of Estonia, 'Address by the Minister of Defence Margus Hanson As Acting Foreign Minister to the Riigikogu 15 June 2004 National Security Concept of the Republic of Estonia (2004)', 15 June 2004, https://vm.ee/sites/default/files/content-editors/web-static/256/MH_NSC_604.pdf.
[94] Ulrich Beck, 'The Terrorist Threat: World Risk Society Revisited', *Theory, Culture & Society* 19, no. 4 (1 August 2002): 41, https://doi.org/10.1177/0263276402019004003.
[95] Ministry of Foreign Affairs of the Republic of Estonia, 'Address by the Minister of Defence Margus Hanson As Acting Foreign Minister to the Riigikogu 15 June 2004 National Security Concept of the Republic of Estonia (2004)'.

becoming for Estonia the most pressing foreign policy priority. Indeed, Erik Männik went as far as to write that Estonia "traded off its openly voiced threat perceptions for Alliance membership candidate status."[96] Such an explanation is also consistent with the previously discussed NATO requirement of prospective members not having tensions with neighbouring countries (a clear reference to Russia) and the hostility of some prominent political voices in the United States towards NATO enlargement to the Baltic states for fear of American embroilment in an unwanted conflict.[97]

The interviews for this thesis confirmed unequivocally that the emphasis on global risks in the 2004 Concept did not accurately reflect Estonia's true security priorities. Instead, what it shows is that there was a deep chasm between Estonia's and NATO's ideas and perceptions of Russia in the 2000s. According to Ilves, the focus on transnational risks in the document was "purely political."[98] "There's this image of the Baltic countries and Poland as being knee-jerk Russophobes," he explained. "And this was at the time of the NATO-Russia Council, *druzhba narodov*, 'we're all friends.'"[99] Estonia in reality had very different security priorities at the time: "We're not stupid," continued Ilves, "we don't have any illusions. We know what's going to attack us. It's been happening for a thousand years. But we assiduously avoided any mention of that [Russian threat] … ."[100]

Aaviksoo further clarified that Estonia "downplayed" the threat of Russia in official documents because the government had "other priorities" – namely, integrating into NATO.[101] Therein lies a paradox that Estonian officials seemed to have skilfully played: addressing the pre-eminent concern over the Russian threat required de-emphasising that threat within alliance circles. While it would not be entirely correct to say that Estonia wanted to "please our future friends and partners," Aaviksoo clarified, "we didn't want to irritate them."[102] According to Riho Terras, former Chief of Staff of the Estonian Defence Forces, "the main issue [about the 2004 strategy] was how it would be digestible to NATO. We wanted to be as good a pupil as possible … the Germans didn't like the word 'Russia' in any of the national strategies."[103] Both Ilves and Aaviksoo affirmed that the 2004 Concept was an attempt to align with NATO's security priorities.[104] Estonia's focus on risks rather than state-based threats in its official national security documents and public statements was therefore a product of wanting to "fit in" at NATO, which in turn was the result of much deeper threat society concerns: the fear of abandonment and constant pursuit of protection from the Russian existential threat.

[96] Männik, 'Small States', 28.
[97] Luik, 'Estonia's Long Road to NATO'; Kennan, 'Opinion: A Fateful Error'.
[98] Author interview with Toomas Hendrik Ilves.
[99] Author interview with Toomas Hendrik Ilves.
[100] Author interview with Toomas Hendrik Ilves.
[101] Author interview with Jaak Aaviksoo.
[102] Author interview with Jaak Aaviksoo.
[103] Author interview with Riho Terras.
[104] Author interview with Toomas Hendrik Ilves; Author interview with Jaak Aaviksoo.

According to Merle Maigre, "deterring Russia has always been the first priority of Estonia."[105] As we discussed, the experience of five decades of Soviet occupation was still prominent in the nation's historical memory.[106] Estonians were firmly focused on Russia and what they already perceived to be the Kremlin's expansionist and revisionist intentions in the international system, especially in its relations with formerly captive nations.[107] But Estonian policymakers were also keenly aware of the much warmer attitudes towards NATO's former adversary in Brussels and Berlin.[108] And their utmost priority was earning and then retaining the commitment of NATO allies.

What were the NATO priorities that Estonia wanted to align with and where did they come from? In 2002, Christopher Coker wrote that NATO was no longer a "security community," but a "risk community."[109] After the disappearance of the Soviet adversary against which the alliance had built up its identity, the void was filled by the alliance's increasing attention to so-called "non-traditional" security issues.[110] In a clear indication that the focus of NATO had shifted from territorial defence in the face of familiar, state-based threats to the management of largely unforeseeable and unquantifiable risks, the kind that preoccupy risk societies most, the 1991 NATO Strategic Concept explained: "[i]n contrast with the predominant threat of the past, the risks to Allied security that remain are multi-faceted in nature and multi-directional, which makes them hard to predict and assess."[111] NATO's strategic documents also indicated a heightened awareness of the negative side effects of modernisation and technological progress, a concern endemic to risk societies: "[t]he global spread of technology that can be of use in the production of weapons may result in the greater availability of sophisticated military capabilities, permitting adversaries to acquire highly capable offensive and defensive air, land, and sea-borne systems … ."[112] Demonstrating a specific preoccupation with the unintended consequences of

---

[105] Author interview with Merle Maigre.
[106] For a detailed analysis of Estonia's historical memory see: Meike Wulf, *Shadowlands: Memory and History in Post-Soviet Estonia* (New York: Berghahn Books, 2016).
[107] On Russian revisionism see: G. John Ikenberry, 'The Illusion of Geopolitics: The Enduring Power of the Liberal Order Essay', *Foreign Affairs* 93, no. 3 (2014): [i]-91; Walter Russell Mead, 'The Return of Geopolitics: The Revenge of the Revisionist Powers Essay', *Foreign Affairs* 93, no. 3 (2014): [i]-79; Fiodor Loukianov, 'Russia, a Revisionist Power?', *Politique Étrangère* 80, no. 2 (Summer 2015), https://www.ifri.org/en/publications/politique-etrangere/articles-de-politique-etrangere/russia-revisionist-power.
[108] Author interview with Toomas Hendrik Ilves.
[109] Coker, *Globalisation and Insecurity in the Twenty-First Century*, 66. Similarly, in 1999, Wallander and Keohane argued that "[t]he NATO that is expanding … is not the old NATO – an alliance focused on threats from the Soviet Union." Rather, they argued, after the threat of the Soviet Union disappeared, NATO transformed into a security management institution concerned with the management of risks. See: Celeste Wallander and Robert Keohane, 'Risk, Threat, and Security Institutions', in *Imperfect Unions: Security Institutions over Time and Space*, ed. Helga Haftendorn, Robert Keohane, and Celeste Wallander (Oxford: Oxford University Press, 1999), 89, 107.
[110] Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London; New York: Routledge, 2010), 2.
[111] NATO, 'Towards the New Strategic Concept: A Selection of Background Documents' (NATO Public Diplomacy Division, April 2010), 22, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120412_Towards_the_new_strategic_concept-eng.pdf.
[112] NATO, 36.

advancements in information technologies, in alignment with the expectations of the risk framework in Chapter 2, the 1999 Strategic Concept warned that, "state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems."[113]

Entwined with the increasing focus on transnational risks was the changing relationship with Russia, the primary security threat against which the alliance had been built. In 2001, two months after the attacks of 9/11, British Prime Minister Tony Blair proposed a Russia-North Atlantic Council in order to build a closer partnership with the Kremlin, involving issues such as peacekeeping in the Balkans and addressing the proliferation of weapons of mass destruction.[114] Other NATO members were also in the process of extending a hand towards Moscow: George W. Bush famously judged that Putin was trustworthy having "looked the man in the eye" and got "a sense of his soul"[115]; Germany was also in the process of building a "special relationship" based on increased trade with Russia.[116] After the NATO-Russia Council was finalised at a meeting in Reykjavik in 1992, Jack Straw, the UK Foreign Secretary at the time, proclaimed "the funeral of the cold war," calling Russia a "friend and ally."[117]

None of this is to say that the NATO allies always unanimously agreed on how to deal with the new security environment. Recall from Chapter 2 that the perception of risks is mediated by individual states' cultural inclinations and historical experience. While relations with Russia improved, the aftermath of the terrorist attacks of 9/11, particularly the transatlantic crisis over the intervention in Iraq, exposed how the different political cultures of alliance members manifested themselves in differing views on how to manage risks and "what if" scenarios.[118] According to Coker, it is in the very nature of a risk community to disagree as "[r]isks only suggest what should *not* be done rather than what should be done."[119] Thus there is more disagreement in a risk community than in a threat alliance because "threat relies … on more concrete evidence and quantification than does risk."[120] The chapter will return later to the discussion about NATO cooperation in the face of cyber risks specifically; but first, having now established the full context of both Estonia's and NATO's defence postures, we turn to the reasons why Estonia decided not ask NATO for a formal response to the 2007 cyber attacks.

---

[113] NATO, 36.
[114] Richard Norton-Taylor, 'Blair Sees Security Role for Russia', The Guardian, 17 November 2001, http://www.theguardian.com/world/2001/nov/17/russia.afghanistan.
[115] 'Flashback: President Bush on Putin's "Soul"', NBC News, 27 March 2014, https://www.nbcnews.com/video/flashback-president-bush-on-putins-soul-208352323648.
[116] Norton-Taylor, 'Blair Sees Security Role for Russia'.
[117] Ian Traynor, 'Russia and Nato Reach Historic Deal', The Guardian, 15 May 2002, http://www.theguardian.com/world/2002/may/15/russia.iantraynor2.
[118] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 6–7.
[119] Coker, *Globalisation and Insecurity in the Twenty-First Century*, 75.
[120] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 37.

6.3.4 Estonia's rejection of meaningful punishment: appeasing the risk community

In April and May 2007, the NATO alliance reckoned with the prospect of Estonia invoking at least one of the articles of NATO's Washington Treaty; the Estonian DDoS attacks were only the second time in the history of the alliance, the first being 9/11, that immediately instigated a discussion among its members about their possible invocation.[121] One NATO official even noted that the attacks went to "the heart of the alliance's modus operandi."[122] Two particular articles would have formally bound NATO's members to address Estonia's situation: Article IV, which we already discussed, and Article V, NATO's famous collective defence clause, which stipulates that an armed attack against one ally is an attack against them all.[123] Ultimately, of course, neither article was invoked and nor – based on what we can observe from the archival record and interviews – was a response to the attacks debated in any formal NATO capacity.[124]

The question that arises is: why did Estonia not lean on NATO for support during and immediately after the cyber attacks? Regarding Article V, Aaviksoo clarified that neither he, nor the government more broadly, saw the attacks as an act of war.[125] Thus, the provisions of Article V did not "automatically extend" to Estonia in this case because the article explicitly references "armed attack."[126] Let us therefore explore why Estonia did not initiate consultations under Article IV or seek a different meaningful response through NATO.

From the beginning, Estonian policymakers had the impression that the alliance was not willing to get involved in the issue of the attacks. Tiido recounted that, "the Secretary General, Jaap de Hoop Scheffer, pulled me aside after one meeting and asked whether Estonia intends to invoke any of the articles, meaning five or four. And it seemed to me he was quite relieved when I answered that we had no intention of doing it."[127] Tiido got the impression that the attitude among the allies was "sceptical" as to the attribution of the attacks to Russia. "In a way, some of them wanted to kind of sweep it aside."[128] Ilves went even further, starkly demonstrating the clash of ideas and perceptions of Russia between NATO and Estonia: "No one believed us … we were told don't even think of an Article IV. … You little east European Russophobes, don't even bother."[129]

The president's emphatic statement betrays a second important Estonian sensitivity: Estonia believed that NATO saw Estonia as inherently hostile towards Russia and therefore troublesome for an

[121] Kello, *The Virtual Weapon and International Order*, 186; Author interview with Jaak Aaviksoo.
[122] NATO official quoted in: Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'.
[123] NATO, 'The North Atlantic Treaty'.
[124] Author interview with Harri Tiido.
[125] Author interview with Jaak Aaviksoo.
[126] Jaak Aaviksoo quoted in: Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'.
[127] Author interview with Harri Tiido.
[128] Author interview with Harri Tiido.
[129] Author interview with Toomas Hendrik Ilves.

alliance that was trying to avoid tensions with the Kremlin. This belief only fuelled Estonia's anxiety about the strength of the alliance's commitment in a future moment of need. Estonia's decision not to pressure the alliance for a response was therefore a product of Estonia's enduring desire to preserve the goodwill and support of the NATO allies in the event of a future Russian invasion. "You can only call the wolf once," explained Maigre. "You don't want to appear as the ally whose hair is on fire … [the] ally who constantly warns everybody or cries about Russia." Instead, Maigre affirmed, you want to be seen as "a normal ally that can care about the security of others, that cares about terrorism, that contributes to the overall international operations in Afghanistan and Iraq."[130] Thus, the decision not to pressure NATO for a response was intertwined with Estonia's desire to "fit in" at NATO and its threat society identity, in particular the fear of being abandoned by NATO at the feet of a menacing historical occupier.

There is more evidence pointing to the same conclusion. Explaining how the issue of the Bronze Soldier had set off the 2007 crisis, Aaviksoo revealed that the Estonian government had previously tried reach a compromise with Russia on the monument to no avail. Although "a symbol of Soviet occupation was standing in the city centre of Tallinn…we thought, OK, it's part of our history, let's leave it there," he explained. "But what turned out is that, starting from 2002, this monument was used as a focal point of anti-Estonian protests [by Estonia's Russian ethnic minority], deliberately so." The Estonian government therefore decided to relocate the monument because, recounted Aaviksoo, "we had intelligence that in exactly 2007 the ultimate goal of those planned protests on the 9th of May, as the celebrations go in Russia, was to reach a point of bloody conflict."[131] Demonstrating the depths of Estonia's concern about the Russian threat, Aaviksoo explained that Russia clearly had "an imperial ambition" to show Estonia "who's boss."[132] But Estonia believed that its western allies did not seem to understand the pressures that the country was under: a leaked diplomatic cable from the time of the attacks reveals that Estonian officials were frustrated by the fact that "Europe's complicated history" was preventing European countries from acting with one voice towards Russia and clouding their judgement of Russia's strategic objectives.[133] According to Ilves, "since they knew nothing about DDoS [attacks], they took as proof that these attacks came from all over – 'why do you say it's the Russians?'," they asked.[134]

NATO's reluctant attitude was further confirmed to the Estonians when Estonia sought practical assistance during the attacks. "One of the things we wanted to do," explained Almann, "was to ask for backup hosting of our government websites – the [websites of the] Ministry of Foreign

[130] Author interview with Merle Maigre. Maigre added that now Estonians are "more comfortable saying it [that they are concerned about Russia] out loud."
[131] Author interview with Jaak Aaviksoo.
[132] Author interview with Jaak Aaviksoo.
[133] U.S. Embassy in Estonia, 'Estonia: GOE Officials on the Bronze Soldier, Russia and Integration'.
[134] Author interview with Toomas Hendrik Ilves.

Affairs, the President, and maybe the Ministry of Defence, [and the] government briefing room." The answer from Estonia's NATO partners was "unanimously negative."[135] Why so? "Because nobody wanted the attack to be directed against their country [too]," explained Almann.[136]

According to Aaviksoo, some countries did ultimately provide Estonia with informal assistance by shutting down the attacks that were being routed through their territories, but much of this support "depended on the risk that [a concrete person – a minister or other decision-maker] was willing to handle."[137] What sort of risks were the NATO allies worried about? The risk of reacting "too harshly against Russia" and escalating a conflict, surmised Tiido.[138]

Given NATO's reluctance, why did Estonia then not decide to respond unilaterally? Again, the concern about remaining in NATO's favour permeated Estonia's threat society reasoning. According to Aaviksoo, who was one of the members of the government that argued against issuing a unilateral response to the 2007 attacks, "[w]e would rather go from sympathy with our friends than … [unilateral] counterattack where there is always less sympathy."[139]

Thus, Estonia's lack of response to Russia through NATO was a result of two intertwined factors: first, NATO's nature as a risk community meant that it was unwilling to support Estonia at the risk of misattribution and escalating tensions with Russia and, second, Estonia decided not to apply pressure for a response for fear of straining its relations with the allies, which it believed might result in abandonment in a future crisis. Importantly, Estonia's concerns, while grounded in reality, were significantly magnified as a result of its threat society identity.

Let us now discuss NATO's cyber risk sensitivity in more detail. Given NATO's identity as a risk community, it is unsurprising that the alliance reacted to the Estonian cyber attacks with extreme caution. The reasons for NATO's reluctance to offer Estonia political and technical support can be summarised as follows: the allies' combined concerns about the risk of the attacks' plausible deniability, the risk of escalation of tensions with Russia, and the risk of unintended effects on their own digital systems. As Chapter 3 discussed, all three of these concerns are characteristic of risk societies, which are highly attuned to potential unintended effects and blowback from their own actions and, more specifically, regard cyberspace as a highly uncertain and unpredictable operational environment, prone particularly to unanticipated blowback, escalation, and collateral effects.

In 2007, such concerns were compounded due to the lack of maturity in NATO's thinking on cybersecurity, which was, in turn, in large part the result of still rudimentary understandings of the technical features of the cyber domain by policymakers and diplomats.[140] Indeed, at the time, NATO

[135] Lauri Almann speaking in: Center for Strategic & International Studies (CSIS), *10 Years of Cyber Estonia*.
[136] Lauri Almann speaking in: Center for Strategic & International Studies (CSIS).
[137] Author interview with Jaak Aaviksoo.
[138] Author interview with Harri Tiido.
[139] Author interview with Jaak Aaviksoo.
[140] Author interview with Merle Maigre; Author interview with Harri Tiido.

had no formal or even informal agreements or procedures for handling major cyber attacks against its member states.[141] The uncertainties regarding the implications of various decisions were thus imbued with what sociologist Frank Furedi described as "Western society's culture of fear," which meant that "possibilistic thinking," "invit[ing] speculation about what can possibly go wrong," [142] became dominant and resulted in the avoidance of decisive action. Instead of responding to Russia, NATO passively sent experts to Tallinn to "observe and provide a summary of the attacks and the GOE [Government of Estonia] response."[143] In a classic demonstration of risk society thinking, the allies were more concerned about the potential unintended consequences of their own actions than about sending a signal of resolve to Russia – in short, risk management logic prevailed over deterrence logic.

Looking at NATO's later efforts in the realm of cyber conflict, which after the 2007 attacks was given significantly more attention by the allies thanks to Estonia's efforts in elevating the issue, it also becomes clear that, in alignment with the risk framework, the alliance continued to see the cyber operational environment as highly uncertain and viewed its operational characteristics as an obstacle to potential meaningful responses. Referring to the risk of misattribution, for example, one of the first NATO documents published on cyber defence, drawing from the Estonian experience of Russian hacker groups working in support of the Kremlin, stated that a "larger crisis" could be "precipitated by the misidentification of an alleged hacker." It went on to caution that "cyber warfare experts have envisaged the accidental war scenario for a number of years."[144] In a demonstration of what Heng called "reflexive rationality,"[145] NATO Secretary General Jens Stoltenberg pointed to the "dark side to this [cyber] technology" and explained to the 2018 Cyber Defence Pledge Conference that "[n]owhere is the 'Fog of War' thicker than it is in cyberspace."[146] Further revealing NATO's view that the attribution problem posed an obstacle to meaningful responses, the 2020 NATO cyber doctrine (the alliance's first ever cyber strategy document) stated that, "despite technological developments, many incidents are likely to be deniable and some untraceable … Non-attributable attacks increase uncertainty and misperception, and thus lead to a perceived reduced political risk and a reduced opportunity for response."[147] The same

[141] Author interview with Jaak Aaviksoo.
[142] Frank Furedi, 'Precautionary Culture and the Rise of Possibilistic Risk Assessment', *Erasmus Law Review* 2, no. 2 (November 2009): 198, 205.
[143] U.S. Embassy in Estonia, 'USG Support for Estonian Cyber Center (Corrected Copy - Added Addressee)', Wikileaks Public Library of US Diplomacy (Tallinn, Estonia: U.S. Embassy in Estonia, 7 February 2008), https://wikileaks.org/plusd/cables/08TALLINN54_a.html.
[144] Sverre Myrli, 'Sub-Committee on Future Security and Defence Capabilities: NATO and Cyber Defence', NATO Parliamentary Assembly, 24 November 2009, 3–4, https://www.nato-pa.int/document/2009-173-dscfc-09-e-bis-cyberdefence-myrli-report.
[145] Yee-Kuang Heng, *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*, Contemporary Security Studies (London; New York: Routledge, 2006), 13.
[146] NATO, 'Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole Militaire, Paris)', NATO, 15 May 2018, http://www.nato.int/cps/en/natohq/opinions_154462.htm.
[147] NATO, 'Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations' (Brussels: NATO Standardization Office, January 2020), 6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

doctrine even dedicated a section to risk management, where it referred specifically to the risk of unintended effects, including collateral damage, blowback, and escalation arising from one's own actions: "COs [cyber operations] can create undesired effects on our own forces and other entities … Differences in the reaction to COs and their effects can become a risk, as it can be difficult to assess how the affected parties perceive activity in or through cyberspace. The risk of escalation should be considered and managed."[148] From these excerpts, it is clear that NATO primarily considered the challenge of cyber attacks through the uncertainty of the cyber operational environment, indicating the extent of its risk sensitivity.

In terms of inter-allied cooperation, the emergence of cyber conflict proved to be a particularly difficult challenge for the NATO risk community to navigate. As Ilves once wrote, the alliance is a defence organization "in a geographical space, constrained inter alia by tank logistics, bomber ranges, [and] the placement of troops."[149] Yet, the insignificance of geography and distance in cyberspace and the fact that states' cyber capabilities do not easily lend themselves to quantitative estimation, partly due to their non-physical nature and partly due to their constant innovation as a result of a continuously shifting attack surface, means that there is much room for subjective interpretation of which states are considered highly capable and what constitutes a risk and what does not.[150] As Coker noted, "[w]hether we think [risks] significant or not, or see them as long-term or short-term, will rest on judgements of their potential."[151] For an intergovernmental alliance of states operating on the basis of unanimity, even small differences in security cultures mean that deliberations on the potential of risks and how to manage them become susceptible to disagreement. As Michael J. Williams showed in the case of NATO's intervention in the Balkans in 1999, although the allies broadly agreed on the nature of the risk in Kosovo, they clashed on the way in which it was to be managed, including on the selection of bombing targets and the use of ground troops.[152] In the case of the intervention in Iraq, the disagreement between the Anglo-American and Franco-German camps on how to manage the risk of the regime of Saddam Hussein developing weapons of mass destruction, and the potential scenario of these falling into the hands of terrorists, catapulted the alliance into perhaps its most serious crisis in history.[153]

Similar disagreements on how to manage cyber risk intensified in the alliance in 2010 prior to the Lisbon Summit. The United States was keen to implement "active cyberdefence," or "pre-emptive

---

[148] NATO, 25.
[149] Toomas Hendrik Ilves, 'A Digital Defense Alliance', *Berlin Policy Journal* (blog), 10 January 2018, https://berlinpolicyjournal.com/a-digital-defense-alliance/.
[150] Erica D. Borghard and Shawn W. Lonergan, 'Why Are There No Cyber Arms Control Agreements?', *Council on Foreign Relations Net Politics* (blog), 16 January 2018, https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.
[151] Coker, *Globalisation and Insecurity in the Twenty-First Century*, 73.
[152] Michael J. Williams, '(In)Security Studies, Reflexive Modernization and the Risk Society', *Cooperation and Conflict* 43, no. 1 (2008): 60, https://doi.org/10.1177/0010836707086737.
[153] Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, 91.

cyber-strikes," while a number of European allies exhibited reluctance.[154] To this day, NATO allies also do not agree on the terms on which individual states' cyber commands can access the systems and networks of allies to disrupt adversarial operations, which has become a particularly pertinent issue since the United States introduced the strategy of persistent engagement and defend forward, a strategy which, as we discussed in Chapter 4, foresees precisely such activities.[155] In 2018, Ilves wrote that while NATO had recognised cyber operations as a security issue (for example by declaring cyberspace to be a military domain at the 2016 Warsaw summit),[156] there had been little operational progress or inter-allied cooperation on the matter.[157] In an interview for this research, he elaborated further: "[a]bout ten years ago we discovered a Russian worm in our military network and we went to NATO and said 'look we discovered this Russian worm.' The answer from NATO was: 'oh, you too!' – which is not the answer you're supposed to get from NATO. It's exactly the opposite [of what one would expect within a collective defence framework]."[158] As the next section will demonstrate, like in 2007, differences in the estimation of threats and risks within the alliance in subsequent years often proved to be challenging for the Estonian threat society, which continued to focus its attention on Russia.

6.4 Estonia in the cyber domain after 2007: a threat society still absorbed by Russia

In the aftermath of the 2007 attacks, we might expect that Estonia would have become more sensitive to the risks that preoccupy risk societies. After all, as the risk framework discussed, states tend to move up the risk spectrum after experiencing surprise events (such as the terrorist attacks of 9/11), especially if they already have certain cultural dispositions (for example, a deeply engrained aversion to civilian harm). There are compelling reasons why Estonia could have become more risk-focused: the attacks might have demonstrated to Estonia its asymmetric vulnerability in cyberspace and raised the awareness of Estonians that technological progress and the conveniences of a digital society come at a steep price. As Linton Wells III, a senior US Department of Defence official, stated at the time of the attacks, "[t]his may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society."[159] Another reason for adopting a more risk sensitive mentality could have been socialization into the NATO risk community, defined as the process of "inducting actors into the norms and rules of a given community," which has the power to alter members' "interpretations of the

[154] Valentina Pop, 'US Call for Nato Cyber-Strike Capacity Causes Division', *EU Observer*, 5 October 2020, https://euobserver.com/news/30962.
[155] Max Smeets, 'NATO Allies Need to Come to Terms With Offensive Cyber Operations', Lawfare, 14 October 2019, https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations.
[156] Jeppe T. Jacobsen, 'Cyber Offense in NATO: Challenges and Opportunities', *International Affairs* 00, no. 0 (31 March 2021): 1, https://doi.org/10.1093/ia/iiab010.
[157] Ilves, 'A Digital Defense Alliance'.
[158] Author interview with Toomas Hendrik Ilves.
[159] Wells quoted in: Landler and Markoff, 'Digital Fears Emerge After Data Siege in Estonia'.

world."[160] Contrary to such expectations, however, we will see that, although Estonia's cyber strategy and adoption of risk management practices seemed to indicate a shift up the risk spectrum, the country in fact remained firmly focused on the Russian existential threat, which forestalled its transformation into a risk society.

After the 2007 attacks, Estonia released its first national cyber security strategy, which, much like in the case of the 2004 National Security Concept, appeared at first glance to indicate the presence of risk thinking. Most notably, it reflected the three main characteristics of risk societies: reflexivity, the preoccupation with risks, and the emphasis on proactive strategies to manage them. Let us therefore first analyse these three key characteristics of risk societies against Estonia's thinking about the cyber domain after the 2007 attacks.

Estonia's first cyber security strategy demonstrated a strong awareness of the negative implications of technological progress, an indication of reflexive thinking, highlighting that, although "[t]he development of Estonia's information society … has been an important driver of the country's spectacular economic growth," the 2007 attacks "demonstrated that the vulnerability of a society's information systems is an aspect of national security in urgent need of serious appreciation."[161] Such a realisation is in line with Beck's account that risk societies develop from a condition of wealth and technological advancement, once society becomes consumed with the unpredictable risks that such advancement can breed.[162]

The 2008 Estonian cyber strategy also emphasised the operational environment's characteristics, particularly its complex adaptiveness, and highlighted the potential risks and worst-case scenarios arising from the nature of the domain. "The damage [from a cyber attack] may be substantial owing to the high degree of interaction between computer networks and also the interdependence of services related to the information infrastructure," it stated. Furthermore, "[f]ailures of or disruptions to critical information systems may impact excessively upon the normal functioning of society with unforeseen and *potentially* disastrous consequences [emphasis added]."[163] The strategy repeatedly

---

[160] Alexandra Gheciu, 'Security Institutions as Agents of Socialization? NATO and the "New Europe"', *International Organization* 59, no. 4 (2005): 973–76. There exists a well-established literature on NATO's collective identity and its influence on new members' understandings of the security environment: Thomas Risse-Kappen, 'Collective Identity in a Democratic Community: The Case of NATO', in *The Culture of National Security*, ed. Peter Katzenstein (New York: Columbia University Press, 1996), 357–99; Wallander and Keohane, 'Risk, Threat, and Security Institutions'; Gheciu, 'Security Institutions as Agents of Socialization?'; Helene Sjursen, 'On the Identity of NATO', *International Affairs* 80, no. 4 (2004): 687–703; Michael C. Williams and Iver B. Neumann, 'From Alliance to Security Community: NATO, Russia, and the Power of Identity', *Millennium* 29, no. 2 (1 June 2000): 357–87, https://doi.org/10.1177/03058298000290020801.

[161] Ministry of Defence of the Republic of Estonia, 'Cyber Security Strategy 2008-2013', 2008, 6–12, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en.

[162] Ulrich Beck, Anthony Giddens, and Scott Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity Press, 1994), 3.

[163] Ministry of Defence of the Republic of Estonia, 'Cyber Security Strategy 2008-2013', 10.

referred to potential scenarios: the potential of human casualties arising from cyber attacks and the potential of the "domino effect" whereby "a failure in one component leads to the failure of others … with serious *potential* consequences [emphasis added]."[164] Recall that a focus on potential harms, which are neither quantifiable nor fully predictable, is one of the chief features of a risk society.

As Chapter 3 outlined, the realisation that "risk problems" have "no unambiguous solutions" leads risk societies to adopt risk management practices (resilience-building, managing consequences, and preventive action).[165] In another seeming indication of a move up the risk spectrum, Estonia after 2007 introduced several such initiatives. In 2018, the Estonian defence forces launched a cyber command whose mission was to engage in, among other things, "active cyber defense operations," or what the risk framework referred to as preventive action.[166] When US Cyber Command deployed to Estonia in a "hunt forward" mission in September 2020 to gain a deeper understanding of Russian cyber campaign tactics prior to the US presidential elections, the Estonian Command sought to learn how the United States implements its preventive operations to disrupt adversary activity (under persistent engagement), further indicating an interest in implementing similar strategies.[167] The exercises also gave Estonia an "independent assessment" of the security of its own networks, thus contributing to the practice of resilience-building.[168]

A second important initiative, which contributed to both the practices of increasing resilience and consequence management, was the creation of a Cyber Defence Unit (CDU) within the voluntary Estonian Defence League (*Kaitseliit*). The unit was developed in order to bolster cooperation and information sharing between information security professionals in the public and private sectors and, in the case of a crisis, help manage the consequences of an ongoing incident by deploying members, including specialists from companies like Skype and Microsoft,[169] to join the incident response team in

---

[164] Ministry of Defence of the Republic of Estonia, 10–11.
[165] Wolfgang Bonss quoted in: Ulrich Beck, Anthony Giddens, and Scott Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity in association with Blackwell, 1994), 9.
[166] Piret Pernik, 'Estonian Cyber Command: What Is It For?', ICDS, 26 November 2018, https://icds.ee/en/estonian-cyber-command-what-is-it-for/.
[167] Shannon Vavra, 'Cyber Command Deployed Personnel to Estonia to Protect Elections against Russian Threat', CyberScoop, 3 December 2020, https://www.cyberscoop.com/cyber-command-deployed-estonia-russia-2020-elections-hunt-forward/; Eric Tucker, 'US, Estonia Partnered to Search out Cyber Threat from Russia', AP NEWS, 3 December 2020, https://apnews.com/article/hacking-russia-estonia-e931e674091b080f7a01642b01729bbe; ERR News, 'Estonia and US Joint Operation Strengthens Cyber Defense', ERR.ee, 4 December 2020, https://news.err.ee/1196470/estonia-and-us-joint-operation-strengthens-cyber-defense.
[168] U.S. Cyber Command, 'Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation', U.S. Cyber Command, 3 December 2020, https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.
[169] Lionel Oh, 'Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia', *Cornell International Affairs Review* 12, no. 2 (2019): 145.

the affected organisation.[170] In a national emergency situation, these individuals also stand ready to be called upon for their expertise and support to the government in mitigating damage to digital infrastructure.[171]

Having analysed the possible indicators of Estonia's move up the risk spectrum after the 2007 cyber attacks, let us now turn to Estonian security thinking after them: did the country, despite the introduction of risk-sensitive cyber strategies and initiatives, nevertheless retain its threat society identity?

In the years after the attacks, alongside the awareness of the pitfalls of technological progress, Estonian policymakers, perhaps paradoxically, developed a striking confidence in the country's cyber defences and the resilience of ever-expanding digital infrastructures (with prominent new initiatives such as "e-residency" coming into being[172]). The 2019 Cyber Strategy, for example, noted particularly that as a result of the 2007 attacks and a vulnerability discovered in the chips of Estonian ID cards in 2017, Estonia had a "one of a kind opportunity to learn lessons from unprecedented cyber crises."[173] Far from creating a crisis of trust among citizens, the Estonian government believed that Estonians, over time, *gained* trust in Estonia's digital infrastructures because both the 2007 and 2017 incidents were successfully resolved.[174] Thanks to investments in cyber defences and the widespread replacement of legacy IT systems, Estonia also did not experience the kind of destruction wrought in other countries by ransomware and wiper operations; for example, it was not affected by WannaCry or NotPetya (the latter touched only multinational companies whose parent networks outside Estonia had been infected).[175] Confidence in the defences and resilience of Estonia's networks thus seemed to offset Estonia's reflexive realisations of the negative side effects of modernization and progress (that are characteristic of risk societies).

But there was a more important factor which meant that Estonia did not turn into a risk society. Its perception of Russia as an existential threat remained and even intensified after Russia's annexation of Crimea in 2014. Already directly after the 2007 cyber attacks, having accepted that NATO was not

[170] Monica M. Ruiz, 'Is Estonia's Approach to Cyber Defense Feasible in the United States?', War on the Rocks, 9 January 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.
[171] Oh, 'Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia', 145; Kadri Kaska, Anna-Maria Talihärm, and Eneken Tikk, 'Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007', in *International Cyber Security : Legal & Policy Proceedings 2010* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2007), 64.
[172] Nathan Heller, 'Estonia, the Digital Republic', *The New Yorker*, 11 December 2017, https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.
[173] Ministry of Economic Affairs of the Republic of Estonia, 'Cybersecurity Strategy 2019-2022', Ministry of Economic Affairs, 2018, 19, https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.
[174] Ministry of Economic Affairs of the Republic of Estonia, 25.
[175] Kevin Kohler, 'Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations', application/pdf (ETH Zurich, 2020), 6–7, https://doi.org/10.3929/ETHZ-B-000438276; Author interview with Heli Tiirmaa-Klaar, 30 March 2021.

prepared to issue a response to Russia, Estonian officials cautioned their allies that "strict talk with Russia … and a strong position [is] the only thing the Russians understand."[176]

In a telling sign of the extent of Estonia's continued anxiety about Russia, the Estonian Foreign Intelligence Service (*Välisluureamet*)[177] devoted the majority of its very first published assessment of Estonia's security environment in 2016 entirely to Russia and Russia-related issues, a trend which followed in subsequent reports.[178] Even in its treatment of cyber concerns, the 2016 report focused, characteristically for a threat society, on the attacker rather than risks of the operational environment, noting that, "[i]n cyberspace, Russia is the source of the greatest threat to Estonia … ."[179] It is also significant that the decision to issue public yearly intelligence reports describing Estonia's international security environment was a direct result of Russia's 2014 annexation of Crimea and an attempt to shed light on the question on every Estonian's mind: "Is Narva next?" referring to Estonia's largest Russophone border city.[180] Thus, Mikk Marran, the Director General of Estonia's intelligence service, explained in the forward to the 2016 report that "the current policies practiced by the incumbent Russian government are likely to remain the sole external power threatening the constitutional order of the Republic of Estonia in the nearest future."[181]

The 2017 report similarly emphasised that Russia is the only country that could pose a threat to "the independence and territorial integrity of the Republic of Estonia."[182] Not only that, but, in a familiar reminder of Estonia's frustrations in 2007, it conveyed a measure of impatience with other countries for underestimating the Russian threat: Marran wrote in the forward to the 2017 report that he hoped that "Russia's intervention in the US elections and involvement in a (failed) coup attempt in Montenegro served as a wake-up call for the international community."[183]

---

[176] Priit Pallum, Director General for External Economic Issues at the Estonian Ministry of Foreign Affairs, quoted in: U.S. Embassy in Estonia, 'Russian Bear Hug Squeezes Estonian Economy'.
[177] The Estonian Foreign Intelligence Service (Välisluureamet) was, prior to a name change in 2017, called the Estonian Information Board (Teabeamet).
[178] Estonian Information Board, 'International Security and Estonia' (Estonian Information Board Teabeamet, 2016), https://www.valisluureamet.ee/pdf/raport/2016-ENG.pdf; Estonian Information Board, 'International Security and Estonia' (Estonian Information Board Teabeamet, 2017), https://www.valisluureamet.ee/pdf/raport/2017-ENG.pdf; Estonian Foreign Intelligence Service, 'International Security and Estonia' (Estonian Foreign Intelligence Service Välisluureamet, 2018), https://www.valisluureamet.ee/pdf/raport/2018-ENG.pdf; Estonian Foreign Intelligence Service, 'International Security and Estonia' (Estonian Foreign Intelligence Service Välisluureamet, 2019), https://www.valisluureamet.ee/pdf/raport/2019-ENG.pdf; Estonian Foreign Intelligence Service, 'International Security and Estonia' (Estonian Foreign Intelligence Service Välisluureamet, 2020), https://www.valisluureamet.ee/pdf/raport/2020-ENG.pdf; Estonian Foreign Intelligence Service, 'International Security and Estonia' (Estonian Foreign Intelligence Service Välisluureamet, 2021), https://www.valisluureamet.ee/pdf/raport/2021-ENG.pdf.
[179] Estonian Information Board, 'International Security and Estonia', 2016, 46.
[180] Estonian Information Board, 5.
[181] Estonian Information Board, 6.
[182] Estonian Information Board, 'International Security and Estonia', 2017, 4.
[183] Estonian Information Board, 4.

As we discussed previously, Estonia also sought to carve out an international leadership role on cyber issues, a move which can also be seen as an extension of the country's fear of Russian aggression and desire to deter it. Already in 2004, Estonia proposed to host a new NATO Cyber Cooperative Defence Centre of Excellence (CCDCOE) in Tallinn.[184] According to Aaviksoo, during the process of accession to NATO, the Estonian government was asked where it could bring added value to NATO; the decision to specialise on cyber issues and build the centre was Estonia's project to bring that added value.[185] Maigre elaborated that while Estonia had always been very keen to have NATO presence in the form of "boots on the ground" to deter Russia, it realised that in 2004 this was not a realistic prospect. Thus, hosting the centre emerged as an alternative option to achieve some NATO presence in Estonia for the purposes of deterrence.[186] According to Ilves, however, prior to 2007, the NATO allies had not seen the need for the centre; it was only after the attacks that the centre was finally accredited by NATO in 2008.[187] The creation of the CCDCOE was thus a savvy means of turning NATO's risk society concern about technological disruption to the service of Estonia's threat society preoccupation with Russia. Even after the CCDCOE's creation, however, showcasing the continued battle of perceptions of Russia, Tiido noted that the period between 2008 and 2014 was a time of "frustration" for Estonians because the allies still did not believe Estonian warnings about "the Russian issue" despite the fact that Russia had just invaded Georgia and mounted another campaign of DDoS attacks on Georgian networks.[188] Not only that, but, in a demonstration of its risk-sensitive nature, NATO did not agree on calling the centre a "cyber war centre," as Estonia had proposed, opting instead for "cyber defence centre." "In NATO, using the word 'war' was a taboo," explained Tiido.[189]

Once Estonia's enduring preoccupation with Russia as an existential threat is taken into account, the country's apparent engagement in risk management practices also emerges in a new light. Let us start with preventive action. While for the United States, cooperation with allies in "hunt forward" missions as part of the strategy of persistent engagement and defend forward was, first and foremost, part of an effort to strengthen the security of US networks and degrade adversary capabilities by exposing their malware and revealing indicators of compromise (thus preventing and mitigating attacks), Estonia saw its cooperation with the United States, and the public announcement of the initiative,[190] as yielding a different, more strategic benefit: sending a deterrent message to Russia.[191]

---

[184] U.S. Embassy in Estonia, 'USG Support for Estonian Cyber Center (Corrected Copy - Added Addressee)'.
[185] Author interview with Jaak Aaviksoo.
[186] Author interview with Merle Maigre.
[187] Author interview with Toomas Hendrik Ilves.
[188] Author interview with Harri Tiido.
[189] Author interview with Harri Tiido.
[190] U.S. Cyber Command, 'Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation'.
[191] Julian E. Barnes, 'U.S. Cyberforce Was Deployed to Estonia to Hunt for Russian Hackers', *The New York Times*, 3 December 2020, sec. U.S., https://www.nytimes.com/2020/12/03/us/politics/cyber-command-elections-estonia.html.

Estonian officials were even keen for the United States to permanently station a team of cyber operators in Estonia to reinforce the deterrent.[192]

Similar deterrence calculations were employed by Estonian officials in their decisions to share information about Russian exploits: "[i]f we discover the malicious activity and we share it with the world, our partners, then attacking is more expensive," which changes the adversary's calculus about who they choose to attack, according to Mikhel Tikk, the Deputy Head of the Estonian Cyber Command.[193] The thinking behind the employment of preventive action was not just hardening the defence surface with the aim of stopping attacks from getting through,[194] but rather communicating the strength of the defences to the adversary in an act of psychological dissuasion – that is, deterrence by denial.

Another initiative, which might at first glance seem to fit the definition of resilience-building as a risk management practice, but actually also reveals Estonia's intense preoccupation with Russia, was Estonia's creation of "data embassies" – "virtual embass[ies] for data in a privately-owned public cloud."[195] In 2017, Estonia opened the world's first data embassy, with similar privileges and immunities as diplomatic missions, in Luxembourg.[196] Although proposed in 2013, the idea of the data embassies became a particular point of discussion after the Russian annexation of Crimea in 2014[197]; their creation was in fact underpinned not by a concern about risks, but a specific concern about the threat of a Russian invasion. As Taavi Kotka, Estonia's former Chief Information Officer, and academic Innar Liiv put it, the "threat of cyber-attacks or a situation in which Estonia would be occupied and would lose its independence for an indefinite length of time" motivated a search for "a solution whereby the Estonian state would endure even despite an occupation of its territory."[198] Jaan Priisalu, the Director General of the Estonian Information System Authority at the time, similarly highlighted

[192] Barnes.
[193] Tikk quoted in: Barnes.
[194] According to Yee Kuang Heng, one of the key scholars in the "war as risk management" literature, the risk society is characterised by a "minimalist ethos." What he means by this is that its primary "motive force" is "safety" at the expense of loftier goals or "grand historical purposes," such as the defeat of the Soviet Union during the Cold War. "The value system is largely negative, striving to prevent the worst, rather than achieving something 'good'," wrote Heng. See: Heng, *War as Risk Management*, 34–35.
[195] Kohler, 'Estonia's National Cybersecurity and Cyberdefense Posture', 6.
[196] Nikolai F. Rice, 'Estonia's Digital Embassies and the Concept of Sovereignty', Georgetown Security Studies Review, 10 October 2019, https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/; Bartłomiej Sierzputowski, 'The Data Embassy Under Public International Law', *International & Comparative Law Quarterly* 68, no. 1 (January 2019): 237, https://doi.org/10.1017/S0020589318000428.
[197] Kohler, 'Estonia's National Cybersecurity and Cyberdefense Posture', 6.
[198] Taavi Kotka and Innar Liiv, 'Concept of Estonian Government Cloud and Data Embassies', in *Electronic Government and the Information Systems Perspective*, ed. Andrea Kő and Enrico Francesconi, vol. 9265, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2015), 152, https://doi.org/10.1007/978-3-319-22389-6_11.

Russian aggression as the motivation behind the initiative.[199] The Estonian government thus resolved that it needed to own servers outside of Estonia's territory that would be 100% under the jurisdiction of the Estonian state and available for not only storing backups of data, but also for the operation of critical services, such as the State Gazette (Riigi Teataja), Estonia's online depository of all its legislation, in a crisis situation.[200] In addition to providing the Estonian state with digital continuity in the case of occupation, locating a data centre in a third country raised the potential costs of an attack for the aggressor: a breach of the Estonian Data Embassy would also impinge on Luxembourg's networks.[201] Thus, the project also served a deterrence function.

In sum, while the 2007 cyber attacks at first glance seemed to indicate an increase in Estonia's reflexivity, this was in fact not the case. Although Estonia engaged in preventive action and took resilience-building seriously, it also actively encouraged NATO to develop punitive responses to cyber attacks. According to Heli Tiirmaa-Klaar, Estonia's Ambassador at Large for Cyber Issues, "in the long run, if we fai[l] to find a proper response to cyber attacks, we also fail in our own deterrence policy – so we actually need to work towards [a] proper response framework."[202] More recently, Estonia was also the first nation to publicly advocate for "collective countermeasures" in response to cyber attacks.[203] Explaining that "[a]llies matter also in cyberspace," Estonian President Kersti Kaljulaid stated that "…Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation."[204] Given what this chapter revealed about NATO's reluctance to become involved in responding to the 2007 cyber operations, Kaljulaid's statement is hardly surprising. Gaining the agreement of NATO allies on collective countermeasures could help deter Russia and, in the event of an attack, could ensure that NATO allies would come to Estonia's assistance, thereby avoiding a repeat of 2007.[205]

The most important factor informing Estonia's approach to cyber conflict was and still is its age-old preoccupation with the perceived existential threat of Russia. Indeed, with the data embassy project, Estonia even prepared for a potential territorial invasion and ensured the ability of its

---

[199] Priisalu quoted in: Leo Mirani, 'In Case of a Russian Invasion, Estonia Is Uploading Its Government to the Cloud', Quartz, 29 May 2014, https://qz.com/214694/in-case-of-a-russian-invasion-estonia-is-uploading-its-government-to-the-cloud/.
[200] Kotka and Liiv, 'Concept of Estonian Government Cloud and Data Embassies', 157.
[201] Willem Verdaasdonk, 'Data Embassies: How Estonia Might Pave The Way For Reducing Uncertainty In Cyberspace', *Leiden Security and Global Affairs Blog* (blog), 25 November 2019, https://leidensecurityandglobalaffairs.nl/articles/data-embassies; Sierzputowski, 'The Data Embassy Under Public International Law', 241.
[202] Author interview with Heli Tiirmaa-Klaar.
[203] "Countermeasures are sub-use-of-force actions or omissions by an injured state directed against another state that would themselves violate international law but for the fact that they are being employed within specified parameters to respond to and remedy antecedent breaches of international law against the injured state." See: Gary Corn and Eric Talbot Jensen, 'The Use of Force and Cyber Countermeasures', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 4 June 2018), https://papers.ssrn.com/abstract=3190253.
[204] Kaljulaid quoted in: Michael Schmitt, 'Estonia Speaks Out on Key Rules for Cyberspace', Just Security, 10 June 2019, https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.
[205] Schmitt.

government to operate in exile. This unwavering focus on the Russian threat meant that Estonia, even after the 2007 attacks, preserved its identity as a threat society.

6.5 Conclusion

The objective of this chapter has been to show that the Estonian threat society abided by the customs and pressures of the risk society writ large. Estonia, conscious of NATO sensitivities towards cyber risk and towards any potential conflict with Russia, and keen to preserve NATO's commitment in the case of a larger Russian security crisis, decided not to pressure the alliance to respond to the 2007 cyber attacks. Indeed, so intense was Estonia's threat society identity, particularly its fear of Russia and related anxiety about NATO abandonment, that it felt its only means of ensuring long-term survival was to defer to NATO's risk sensitivities rather than seeking a collective response to the cyber attacks.

The chapter began with describing the scale and costs of the 2007 attacks and showing that the Estonian government regarded them as a national security issue and believed they had been sponsored by the Kremlin. Next, it moved on to discuss the Estonian threat society as a product of Estonia's traumatic historical experience of Russian occupation and its adoption of Finnish strategic culture and Finland's total defence model in the 1990s. The analysis showed that Estonia held a deep-seated preoccupation with Russia as an existential threat even as relations between Moscow and the west improved. Highlighting the extent of Estonia's fear of Russia was its pursuit in the 2000s of a unique national security model of total defence (including conscription) within a collective defence structure. The discussion showed that joining NATO was seen by Estonia as an "existential necessity."[206] The decision to craft its National Security Concept of 2004 to align with NATO's risk focus (at odds with Estonia's true worry about the Russian threat) was, in this sense, a manifestation of the extreme determination to join the alliance, precisely to ensure long-term protection from Russia. Even long after joining, however, Estonia continually feared NATO abandonment and retained compulsory military service, unlike the other Baltic states.

Having established that the roots of Estonia's angst over ensuring the support of NATO lay in the threat society, the chapter proceeded to investigate Estonia's decision not to invoke Article IV or Article V or insist on any formal NATO proceedings over the 2007 cyber attacks. It found that Estonian policymakers had been aware that NATO was reluctant to engage formally on the issue of the attacks due to its sensitivities to risk. Because the Estonian threat society was so wedded to the idea that, in order to maintain the long-term commitment of the allies to defend Estonia in the case of a Russian invasion, the country had to be judicious in selecting the issues it formally brought to NATO *and* demonstrate its alignment with NATO's identity, the Estonian government chose not to put pressure on the alliance to respond.

[206] Weiss, 'The Hero Who Betrayed His Country'.

The chapter also found that NATO's unwillingness to support Estonia on the issue of the cyber attacks as a risk community aligned with the expectations of the risk framework: NATO was worried about the possible risks of Russian plausible deniability, the risk of escalation of tensions, and the risk of unintended effects on allies' own digital systems if it agreed to Estonia's request for backup hosting of its websites. An analysis of NATO's post-2007 engagement with cyber issues also revealed the presence of risk thinking – the alliance paid particular attention to the characteristics of the operational environment and the risks stemming from these when addressing cyber conflict.

The main argument of this chapter also illustrated, once again, the importance of ideational factors in shaping the perception of material realities: the Estonian threat society's preoccupation with the existential threat of Russia, which was closely linked to the fear that NATO might abandon it in an Article V scenario, and the NATO risk community's preoccupation with risks and uncertainty, leading it to worry about escalation risks from responding meaningfully to cyber attacks. Identities and beliefs, in other words, shaped the behaviour of Estonia and NATO to produce the absence of a meaningful response to the 2007 cyber attacks. What is more, the chapter illustrated a continual battle between Estonian and NATO perceptions of Russia over the years: Estonia believed NATO was severely underestimating the Russian threat and NATO saw Estonia as "Russophobic."

In the final section, the chapter observed that Estonia's post-2007 cyber strategy seemed to indicate increased reflexivity, prompting the question of whether, as a result of the attacks, Estonia had moved up the risk spectrum. The subsequent discussion revealed, however, that Estonia's attention remained consumed by the existential threat of Russia. The implementation of several new projects, such as the creation of data embassies, was in fact motivated by Estonia's enduring, and even increased, preoccupation with the threat of a Russian invasion. This thinking distinguishes Estonia from risk societies whose actions are motivated by potential and diverse scenarios, usually not explicitly tied to a single actor perceived as an existential threat. In Estonia's case, the scenario of Russian occupation continued over the years to haunt the imaginations of Estonian decision-makers. Consequently, Estonia emerged as a state balancing between NATO's preoccupation with risks and its own enduring concern with the Russian existential threat.

Chapter 7
Conclusion: Contributions, Policy Implications, and Further Research

7.1 Introduction

This thesis represents the first attempt to adapt and apply the risk society framework to an analysis of the empirical puzzle of state responses to cyber attacks in a way that also contributes new insights for further research and for constructivist theory in International Relations. In applying the framework, the thesis advanced a number of empirical claims. It argued that state responses to cyber attacks stem from societal attitudes towards risk and threat, which are in turn a product of cultural and historical factors. Risk societies that are high on the risk spectrum do not punish cyber attacks meaningfully, while threat societies that are low on the risk spectrum seek to do so. The case studies illustrated that states attach different levels of importance to the characteristics of the cyber operational environment as posing an obstacle to meaningful responses. In the United States, concerns about collateral damage, blowback, and the escalatory potential of the operational environment were paramount in producing weak responses under the two Obama administrations and under the Trump administration. On the other end of the risk spectrum, in Israel, retaliation for cyber attacks was not contemplated with reference to potential risk scenarios that might result from the characteristics of the cyber domain. Rather, Israeli strategic culture and officials' perception of the Iranian existential threat was what created the more risk-acceptant Israeli threat society and produced a willingness to respond meaningfully. Estonia was a more peculiar case. The presence of a risk acceptant posture that was predisposed to meaningful response against its former occupier Russia was largely nullified during the 2007 cyber attacks owing to Estonia's membership of the NATO alliance, a risk community whose risk sensitivities officials in Tallinn respected so as to not jeopardise the alliance's collective defence guarantee in what they perceived to be a plausible future crisis scenario involving Russia. Estonia eschewed a meaningful response not because it was a risk society, but because it was a member of a larger risk community and because, as a threat society, it was entirely consumed with the fear of the Russian threat.

This chapter will first summarise the key findings of the thesis and compare and contrast the empirical case studies on the following topics: the views of the operational environment and escalation, the problem of attribution, and differences in preventive action. Second, it will discuss the theoretical contributions of the thesis to International Relations scholarship. Third, it will turn to the implications of the thesis for cyber studies and for cybersecurity policy. Fourth, it will briefly discuss developments that occurred after the period of investigation of the thesis. The final part of the chapter will suggest avenues for further research.

7.2 Key empirical findings

In the first empirical case study, the thesis observed the reluctance of the United States to impose meaningful costs in return for adversaries' damaging and disruptive cyber attacks, something which became especially clear in the wake of the 2016 election interference. The chapter examined the roots of the US risk society, finding that a combination of shock historical events like 9/11 and cultural factors like casualty aversion led the United States to become particularly sensitive to risks after the end of the Cold War. It was during this time, wrote Coker, that "academics and policy-makers had begun to turn their attention, not to threats that could be deterred … so much as risks that fell 'below the threshold' of deterrence."[1]

The chapter found that, in accordance with the risk framework developed in Chapter 2 and Chapter 3, risk sensitivities precluded a meaningful response. The evidence gathered for this study indicated that, when deciding on a response, US policymakers paid particular attention to the characteristics of the operational environment, especially its complex adaptiveness and the proliferation of cyber capabilities. They were concerned about the risks of misattribution and the risks of unintended consequences of a response, particularly a cyber response, in the form of escalation, collateral damage, or blowback. The United States also implemented risk management practices; preventive action over time became a central pillar of its cyber strategy. The chapter showed that arguments guiding US decision-making with regard cyber conflict were similar to the "preventative defence" thinking adopted by the United States first in the late 1990s, and then after the terrorist attacks of 9/11. The behaviour of the United States in responding to cyber conflict was, in short, consistent with the behaviour of a risk society; the sensitivity to risks stemming from the nature of the operational environment resulted in weak responses to cyber attacks.

The second case study focused on Israel, a country which exhibited a much greater willingness to punish cyber attacks meaningfully. The case study showed that Israeli decision-making processes to respond to cyber aggression were a product of the interplay of material and ideational factors. In particular, three elements of strategic culture, the siege mentality, the problem-solving attitude, and the cult of offensive action, formed the threat society lens through which Israel perceived the material world and formulated its deterrence strategy, which emphasised building a reputation for forceful retaliation and giving the attacker a sense of Israel's superior capabilities. Because Israel did not perceive cyberspace as a strategically distinct domain, this deterrence strategy was applied also to cyber issues. Israel's threat society identity thus produced its reactions to cyber attacks: in devising a response, policymakers focused on their perception of the attacker as an existential threat, believed in the necessity of forceful punishment, and were acceptant of its escalation risks. Unlike risk societies, Israel did not pay attention to the risks stemming from the nature of cyberspace. The chapter illustrated the

[1] Christopher Coker, *War in an Age of Risk* (Cambridge: Polity Press, 2009), 140.

influence of the threat society on Israeli responses using the case of the response to Iran's attack on Israel's water infrastructure. Finally, the chapter discussed Israel's engagement in preventive action, resilience-building, and consequence management. It argued that Israel's preventive action, conducted under the strategy of the campaign between wars, had a deterrence objective and therefore could not be considered a risk management practice. While Israel did engage in resilience-building and consequence management, these practices were not portrayed as strategies intended to address state-level, political cyber conflict.

The third empirical chapter examined the case of Estonia, which chose not to turn to NATO to respond meaningfully to a series of cyber attacks emanating from Russia in 2007. The chapter placed emphasis on Estonia's intense fear of Russian occupation. Even after joining NATO, Estonia retained conscription as part of a "total defence" model and harboured a constant fear of NATO abandonment. In fact, Estonia sought to gain the favour and commitment of NATO allies to such an extent that it even tailored its published national security strategies to align with NATO's preoccupation with transnational risks, neglecting to emphasise its own main concern with the Russian threat (knowing that NATO was cautious about accepting countries that had highly tense relations with Russia). The preoccupation with retaining the goodwill of NATO in the face of a perceived existential threat also played a crucial role in the response to the 2007 attacks. The chapter found that, although Estonia itself (like Israel) was a threat society – the result of a fixation on the Russian survival threat and a fighting spirit inherited from Finnish strategic culture – it eschewed a response to Russia because it was constrained by the awareness of NATO's risk sensitivities and its own concern that if it disregarded these sensitivities, NATO might not come to its assistance in the event of a more serious crisis with Russia. In a manner characteristic of a threat society, Estonia's decisions and actions were guided by the fear of one particular scenario involving one particular state actor: Russian occupation. The chapter ended with an analysis of Estonia's approach to the cyber domain after 2007, finding that although the country seemed to become more reflexive in its awareness of the risks inherent in cyberspace after 2007, its enduring worry about the Russian threat meant that it retained its threat society identity.

It is not a coincidence that both Estonia and Israel adopted strategies of total defence: the choice of this strategy was guided by their desire for self-reliance, which is a core characteristic of threat societies, derived from strategic culture and lessons from history.[2] This feature was particularly underscored by the fact that both maintained total defence even while being supported with significant military aid from the United States. There is, however, a major difference between the two cases pertaining to their level of risk acceptance. Because of Estonia's strong desire to retain the sympathy of its NATO allies, the country could not practice risk acceptance as Israel did. Although Estonian policymakers frequently employed strong rhetoric against Russia, the case study in Chapter 6 showed

[2] Joelle Garriaud Maylam, 'Committee on the Civil Dimension of Security: Enhancing the Resilience of Allied Societies Through Civil Preparedness' (Brussels, Belgium: NATO Parliamentary Assembly, 3 March 2021).

that Estonia had to continually balance between its own focus on the singular survival threat and the sensitivity of NATO to risks, as it perceived the alliance to be its ultimate guarantee of security in the event of an occupation scenario, which permeated all of its decision-making.

Having summarised the findings of each of the individual case studies, let us now draw more specific comparisons between the cases on the following issues: the views of the operational environment and escalation, the cyber attribution problem, and preventive action.

7.2.1 Views of the operational environment and escalation

The analysis in Chapter 3 expected states with a high sensitivity to risks to pay significant attention to the operational features of cyberspace and be unwilling to administer meaningful punishments due to these risks. Conversely, states with a low sensitivity to risks and an overwhelming focus on threats were not expected to perceive the features of the cyber domain and their attendant risks as an obstacle to responses. The starkest contrast in the views of the operational environment and, in particular, concerns about escalation risks, was between the United States and Israel; Estonia itself did not see the operational features of the environment or escalation risks as impeding a meaningful response, but felt it had to pay heed to the risk sensitivities of NATO allies.

Both the Obama administration and the Trump administration in the United States were highly attuned to the features of the operational environment and the risks and worst-case scenarios that these could produce. The technology that had previously spurred enormous economic growth was now regarded as a security risk. The United States, in other words, became highly reflexive in its recognition of the negative side effects of modernisation and technological progress. When deciding on how to respond to cyber attacks, officials voiced concerns about the complexity of cyberspace, its dense interconnections, and the proliferation of malware, which were seen to empower a diverse array of actors. Unpredictability and uncertainty – and therefore risks – were understood by US policymakers to characterise the cyber domain.

The case of Israel, meanwhile, showed that policymakers paid little or no attention to the cyber domain's operational characteristics when deciding on how to punish cyber attacks – this was in line with the expectations of Chapter 3. Israel did not exhibit the reflexivity noted in the United States. On this issue of reflexivity, Estonia was an intriguing case study as Estonia's public documents, particularly its national cyber security strategy, at first glance appeared to indicate that after the 2007 cyber attacks Estonia became more reflexive. A deeper investigation into Estonia's view of the international security environment, however, revealed that, as in the case of Estonia's 2004 National Security Concept, the cyber strategy did not reflect Estonia's most pressing security concern. The analysis found instead that the enduring perception of Russia as a survival threat crowded out concerns about risk, which meant that Estonia did not move perceptibly up the risk spectrum and retained its threat society identity.

Closely related to states' perceptions of the operational environment was the level of attention devoted to the risks of escalation. The analysis in Chapter 3 expected that reflexive risk societies would be especially concerned about escalation risks as a potential unintended side effect of their own response. And indeed, in the United States, policymakers repeatedly referred to the risks of escalation as forming part of their decision calculus on responses. The range of potential scenarios was diverse; as is characteristic of a risk society, US policymakers were not preoccupied with one particular escalation scenario entailing a specific adversary, but rather many potential disasters in relation to the nature of the operational environment.

Meanwhile, Israeli officials emphasised that the risk of escalation resulting from a response must be accepted as part of any offensive action, regardless of the domain. They dismissed concerns about cyber escalation as unnecessarily obstructive because, given Israel's fraught relations with its neighbours, they believed that the risk of escalation was always present and had to be accepted as a part of everyday life. Interestingly, Estonian policymakers conveyed a similar acceptance of escalation risks. For example, in the context of anticipating future conflict in cyberspace, Heli Tiirmaa-Klaar, Estonia's Ambassador at Large for Cyber Diplomacy, explained that, regardless of the actions of Estonia or other states, if Russia wanted to escalate, it would do so. What we see here is that threat societies primarily see escalation as *intentional*, which leads naturally to a primary consideration of the nature of the adversary, rather than the features of the operational domain. By contrast, risk societies are preoccupied by *inadvertent* escalation; they pay more attention to how the operational domain increases the likelihood of misunderstanding and subsequent escalation, rather than to the problem of intentional escalation.

7.2.2 The problem of attribution

The risk framework expected risk societies to worry about the risks of misattribution and plausible deniability; this meant that they would engage in long attribution processes and only communicate their findings publicly once they had achieved high confidence in their judgement. Credibility of attribution was paramount. To further decrease the risk of the adversary plausibly denying their culpability, they would seek support from allies in their public attribution statements. The length of the process was therefore expected to impede the swiftness of their response. Conversely, threat societies, given their risk-acceptant disposition and focus on a single adversary, were not expected to manifest concerns about attribution and its plausibility. Indeed, threat societies would be unlikely to harbour doubts about the identity of their attacker. In the case studies, once again, the largest contrast in dispositions towards attribution was between Israel and the United States; the Estonia case study illustrated how Estonia as a threat society was constrained in standing by its attribution statement, likely by the risk sensitivity of NATO.

In the United States, starting from President Barack Obama's attribution of the Sony Hack in 2014, public attribution became a cornerstone of US responses to cyber attacks. Importantly, public attribution statements were not issued until the United States achieved what it considered to be high levels of confidence in the attacks' perpetrators – the obstacles posed by such long attribution processes were illustrated with the case of NotPetya. By the time the United States publicly attributed the attack, it had run out of time for issuing what could have been considered a meaningful response.[3]

Israel did not subscribe to a policy of public attribution – in fact, as Chapter 5 discussed, Israeli policymakers believed that disclosing the identity of the perpetrator did not serve strategic ends as it impeded swift and decisive retaliation, the need for which was culturally engrained in Israel's threat society identity. Israeli policymakers were also unconcerned about potential escalation risks resulting from misattribution and conveyed a high level of confidence in Israel's technical attribution abilities.[4] The latter may have been a result of Israel's intense, almost myopic, focus on what it perceived as an existential threat – Iran – which meant that the Islamic Republic was always the primary suspect as the perpetrator or sponsor of an attack, leaving little to be gained from providing public evidence of attribution. Finally, attributing an attack was also found to contradict another key belief in Israeli strategic thinking: that Israel must display disproportionate strength over the enemy. Attributing an attack in this context might be viewed as an admission of weakness of Israel's digital defences.

Initially, Estonia also seemed to be unconcerned about the risks of misattribution and plausible deniability. Foreign minister Urmas Paet boldly attributed the 2007 attacks to the Russian government. This statement was, however, subsequently diffused by the defence minister, possibly due to pressure from NATO. We know that Estonia's NATO allies, aligning with the expectations of the risk framework, had noted the difficulty of attribution in the cyber domain; because of this difficulty, they were not convinced that the Kremlin was the definitive sponsor of the attacks and worried about the escalation risks that could result from misattribution. The Estonia case study thus illustrated the different perceptions of the problem of attribution by a threat society, on the one hand, and a risk community, on the other.

7.2.3 Differences in preventive action

According to the risk framework developed in the thesis, risk societies are particularly likely to engage in preventive action as a means of managing the risks of the cyber operational environment (the framework noted that threat societies might also pursue preventive action, but this would be done

[3] Recall from Chapter 1 that swiftness is one of the features that makes a response meaningful.
[4] Roy Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL: Talk!* (blog), 9 December 2020, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; Author interview with Gabi Siboni, 17 December 2020.

alongside reactive strategies and would not serve risk management purposes). The thesis showed that both the United States and Israel engaged in preventive action – under the respective terms of persistent engagement and defend forward (PE and DF) and the campaign between wars (CBW). The major difference between the two approaches was the fact that one was a risk management practice, whereas the other was not: while the US strategy of PE and DF was built on the recognition of cyberspace as a strategically distinct domain and, on a general level, intended to minimise the risks of cyber conflict, Israel saw the CBW as fitting into a broader strategy of deterrence – it was not a strategy designed to meet the particular risks of the cyber domain.

PE and DF notably departed from the previous US strategy's reliance on "threats of prospective action" and "episodic responses" designed to "dissuade and deter."[5] A significant advantage of the strategy of persistent engagement and defend forward was found in its mission to neutralise cyber operations *before* they reach US networks, thus eliminating the need for a punitive response and avoiding the associated risk of escalation, a key concern of the US risk society. The Israeli CBW, meanwhile, was meant to bolster deterrence (in all domains) by building Israel's credibility as a forceful retaliator, demonstrating superiority of force, and weakening the confidence and capabilities of the adversary. Cyber tools were regarded as an additional means of contributing to this effort. Israel's intention was not to meet the challenge of a specific kind of *activity* – its purpose was to postpone and prepare for a future war with a clearly-defined *adversary*. Israeli in the CBW thus relied expressly on offensive action and the use of force and accepted that this strategy of limited war might result in escalation into full armed conflict. In this way, the CBW was also a product of Israel's threat society identity.

Finally, Estonia also showed interest in engaging in preventive action: when US Cyber Command was deployed to Tallinn, the Estonian Command sought to learn from its operations conducted under PE and DF. What the Estonia case study also showed, however, is that Tallinn's motive extended beyond learning techniques to advance Estonia's interests in cyberspace; Estonian officials, consistent with their country's threat society identity, in publicly announcing their cooperation with the United States also sought to send a deterrent message to Russia.

Having discussed the main findings of the thesis and compared and contrasted the case studies, let us now turn to the theoretical contributions of this work.

7.3 Contributions to International Relations scholarship

The inability of rational choice and cognitive theories in International Relations to make sense of the empirical puzzle led the thesis to turn towards constructivist approaches. Its first contribution

[5] Emily Goldman, 'From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy', *Texas National Security Review* 3, no. 4 (Fall 2020): 94.

was therefore to apply a constructivist lens to issues of international cybersecurity, thus expanding the empirical boundaries of constructivism. Despite important work by Finnemore and Hollis,[6] cybersecurity is still an understudied topic within constructivism and has mainly been addressed from the perspective of systemic norm creation. However, systemic or "third-level" constructivism, which explores ideas and beliefs that are common among states, was unable to account for variance in state responses to cyber attacks because shared cyber norms are still at a very early stage of the norm life cycle. Addressing this shortcoming was the second scholarly contribution of this thesis: the thesis developed a conceptual framework based on domestic or "second-level" constructivist approaches, which prioritise the internal culture of states and the ideas and beliefs of countries and regimes (that is, they seek to open up the "black box" of the state). The thesis argued that variation in state responses resulted primarily from differences in national-level ideational characteristics. But that is not to say that material conditions were irrelevant. Rather, adopting Beck's "critical realist" approach, the thesis assumed that material conditions exist independently of perception but take on particular meaning through culture and history. In the case studies we saw how, in the case of the United States, historical and cultural factors, such as casualty aversion, and an increased reflexivity born from events like the surprise attacks of 9/11 and various environmental disasters, meant that the cyber operational environment was seen as uncertain and risky; in the Israel case, elements of strategic culture, itself a product of Israel's difficult history, created Israel's threat society identity and led to a fixation on Iran as an existential threat, despite Israel's overwhelming military superiority over its adversary; in Estonia, a traumatic history of recent Soviet occupation produced an intense threat society focus on the prospect of Russian invasion, even at a time when Russia was not regarded as a threat by the west, which meant that Estonia avoided tensions with its NATO allies and bowed to their risk sensitivities in hope of retaining their collective security guarantee in a future crisis.

The third central contribution of this thesis was conceptual: the thesis refined the concept of the risk society as originally proposed by Beck and introduced the concept of the threat society, which is absent in his framework. Socially constructed risk has been an understudied phenomenon in International Relations.[7] Risk perception in IR has mainly been approached from cognitive and psychological standpoints, such as through Prospect Theory.[8] The approach that this thesis builds on, the risk society theory borrowed over from Sociology, explains that risk aversion arises in some countries as a societal trait due to the interaction between cultural values and technological progress. More specifically, an awareness of the negative side effects of technological progress means that these societies become highly reflexive. The theory of the risk society, with the addition of the concept of the

[6] Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International Law* 110, no. 3 (July 2016): 425–79, https://doi.org/10.1017/S0002930000016894.
[7] William Clapton, 'Risk in International Relations', *International Relations* 25, no. 3 (2011): 280–95, https://doi.org/10.1177/0047117811415480.
[8] Rose McDermott, *Risk-Taking in International Politics: Prospect Theory in American Foreign Policy* (Ann Arbor: University of Michigan Press, 1998).

threat society, thus provided the basis for an explanation for the research puzzle: that societal risk aversion or risk acceptance, a product of historical and cultural factors, shaped different actors' perceptions of how best to pursue their interests in the face of the dangers they perceived.

To fully operationalise the risk framework, the thesis detailed the key features of different societies on the risk spectrum (risk societies, mid-spectrum societies, and threat societies), and, in Chapter 3, based on these features, developed an analysis of how these societies would be likely to perceive the operational characteristics of the cyber domain. Although the cyber operational environment created constant pressures and constraints within the three case studies, the theory expected different states to react to these environmental conditions in starkly different ways, that is, based on their different social risk dispositions. More concretely, the thesis expected that risk societies, highly attuned to operational uncertainty as a result of their cultural and historical experience, would perceive the characteristics of the cyber domain as an obstacle to meaningful punishment and thus issue weak responses to cyber attacks. Threat societies, meanwhile, consumed by their historical focus on a perceived existential threat and culturally risk acceptant, would be unlikely to pay particular attention to the features of the operational environment as a hindrance to forceful responses and therefore punish meaningfully. The framework also expected that risk societies would focus far more on risk management practices as a central means of addressing the challenge of cyber conflict than threat societies.

The fourth major contribution of this thesis was to the "war as risk management" literature within security studies. While that literature concentrated on understanding the motives and conduct of western wars through the lens of socially constructed risk (such as the intervention in Afghanistan and the Iraq war), this thesis extended the inquiry into the area of cyber conflict and specifically to responses to cyber attacks. The thesis also went beyond investigating just risk societies, thereby uncovering the important influence of strategic culture as a crucial determinant of risk acceptance within threat societies confronting a perceived existential threat abroad. By developing clear indicators of a risk society, a mid-spectrum society, and a threat society, the thesis enabled a systematic diagnosis of each state's risk or threat identity in the case studies. Such clear indicators are absent in the war as risk management literature.

7.4 Implications for cyber studies and cybersecurity policy

In addition to the theoretical and conceptual contributions to International Relations, this thesis also sought to contribute to existing scholarly debates in the sub-field of cyber studies and to provide policy-relevant knowledge. One issue that has generated a particularly lively debate in cyber studies has been the question of whether the cyber domain is inherently escalatory or not, which, as we saw, is

a special concern of policymakers in risk societies such as the United States.[9] Ben Buchanan posited that the operational nature of the cyber domain is such that states will, on the one hand, be incentivised to penetrate each other's networks for defensive purposes but, on the other, upon finding an adversary in their networks, find it difficult to distinguish an espionage operation from a sabotage operation. As Chapter 3 discussed, the structural features of the cyber domain enhance the "dilemma of interpretation" faced by a state figuring out how to respond to a hostile operation, which leads to a "dilemma of response."[10] Because states exist in an anarchic, self-help system, the victim's response will try to increase his security, thereby threatening the security of the perpetrator.[11] The primary message of Buchanan's book is a cautionary one: the nature of the cyber domain increases the likelihood of escalation and systemic instability.[12]

The findings of this thesis complicate even more the picture painted by Buchanan. The thesis does not dispute that the operational realities of the cyber domain can have serious implications for state behaviour or that the cybersecurity dilemma might arise due to the nature of the environment. It shows, however, that equally important for understanding cyber-related decision-making are states' culturally influenced perceptions. Thus, it is not difficult to imagine that in the case that Israel detects an Iranian cyber operation in its networks, it will assume the worst intentions and respond forcefully, potentially leading to tit-for-tat escalation. In the case that the United States detects one of its adversaries in its networks, the cybersecurity dilemma may still flare up, but there is a lower likelihood that tensions will escalate significantly given US risk sensitivity. Ideational factors are therefore crucial for understanding the intensity of the cybersecurity dilemma and its escalatory consequences.

---

[9] For examples of scholarly works on cyber escalation see: Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (London: Hurst & Company, 2016); Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *The Cyber Defense Review*, 2019, 267–87, https://doi.org/10.2307/26846132; Erica D Borghard and Shawn W. Lonergan, 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly*, Fall 2019, 24; Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015); Ben Buchanan and Fiona Cunningham, 'Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis' 3, no. 4 (Fall 2020): PDF not yet available; Ronald J. Deibert, 'Bounding Cyber Power: Escalation and Restraint in Global Cyberspace', in *Organized Chaos: Reimagining the Internet*, ed. Mark Raymond and Gordon Smith (Ontario, Canada: Centre for International Governance Innovation, 2014); Jason Healey, 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 15 June 2016), https://doi.org/10.2139/ssrn.2836206; Sarah Kreps and Jacquelyn Schneider, 'Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics', *Journal of Cybersecurity* 5, no. 1 (1 January 2019), https://doi.org/10.1093/cybsec/tyz007; Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), https://www.rand.org/pubs/monographs/MG1215.html; Herbert Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', *Strategic Studies Quarterly* 6, no. 3 (2012): 46–70; Nadiya Kostyuk, Scott Powell, and Matt Skach, 'Determinants of the Cyber Escalation Ladder', *The Cyber Defense Review* 3, no. 1 (2018): 123–34; Christopher Whyte, 'Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online', *European Journal of International Security* 5, no. 2 (June 2020): 195–214, https://doi.org/10.1017/eis.2020.2.

[10] Buchanan, *The Cybersecurity Dilemma*, 20.

[11] Buchanan, 3.

[12] Buchanan, *The Cybersecurity Dilemma*.

Another important debate in cyber studies has revolved around the question of whether deterrence is an appropriate strategy for cyberspace (the fruits of which encouraged the adoption of the aforementioned strategy of persistent engagement and defend forward).[13] Harknett and Fischerkeller showed that the cyber domain is a unique environment of "constant contact" where territorial boundaries that would allow for the declaration of thresholds do not exist, which is a necessary requirement for deterrence to work.[14] Thus, there is a "comprehensive mismatch" between the realities of the strategic environment and the "tactical, operational, and strategic bases of deterrence."[15] They traced the use of weaker forms of punishment in the United States (such as the indictments, sanctions, and public attribution statements) to the fact that deterrence cannot be credibly imposed in cyberspace.[16] Instead of deterrence, the scholars recommended a strategy of cyber persistence.[17] This thesis elaborated on the reasons for weak punishments to show that they were a result of US risk aversion, which influenced policymakers' interpretation of the operational environment as uncertain and risky. The US case study in this thesis revealed that the strategy of persistent engagement aligns closely with US cultural risk sensitivity. In particular, the preventive mission of persistent engagement seeks to manage the risk of surprise attacks and, in prescribing constant operations in foreign networks to disrupt hostile campaigns before they reach home infrastructures, reveals a mindset that is unwilling to accept the occurrence of potentially harmful scenarios.

The most important policy takeaway from this work is therefore that strategies should be adapted to the cultural and ideational context of the state in which they will be implemented. As Bernard Brodie famously warned, "[g]ood strategy presumes good anthropology and good sociology."[18] In the United States, a strategy of meaningful punishment for mid-level cyber attacks (i.e. attacks not falling above the threshold of armed conflict) jars with the culturally and historically engrained concern to manage uncertainty and risk.[19] The strategy of persistent engagement and defend forward is better suited to the risk dispositions of US society.

---

[13] Richard J. Harknett and Joseph S. Nye, 'Correspondence: Is Deterrence Possible in Cyberspace?', *International Security* 42, no. 2 (November 2017): 196–99, https://doi.org/10.1162/ISEC_c_00290; Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61, no. 3 (2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003; Richard J. Harknett, 'United States Cyber Command's New Vision: What It Entails and Why It Matters', Lawfare, 23 March 2018, https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters; Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect', Lawfare, 6 February 2020, https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

[14] Fischerkeller and Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', 385–86.

[15] Fischerkeller and Harknett, 386.

[16] Fischerkeller and Harknett, 387.

[17] Fischerkeller and Harknett, 388–93.

[18] Brodie quoted in: Michael J. Williams, *NATO, Security and Risk Management: From Kosovo to Kandahar*, Contemporary Security Studies (London; New York: Routledge, 2010), 17.

[19] Monica Kaminska, 'Risk Aversion Is at the Heart of the Cyber Response Dilemma', *Council on Foreign Relations Net Politics* (blog), 31 March 2021, https://www.cfr.org/blog/risk-aversion-heart-cyber-response-dilemma.

From the Estonia case study, we can conclude that NATO should consider adopting a similar preventive strategy – a task that would fall to the newly developed NATO Cyber Operations Centre in Mons, Belgium.[20] A re-orientation towards proactive strategies is likely to be enthusiastically welcomed particularly by Estonia, which believes that it depends on the alliance for security and, as a threat society, has in the past quietly harboured frustrations about NATO's posture of relative passivity, both in cyberspace and outside it.[21] While as a threat society Estonia might prefer NATO to implement a strategy of deterrence by punishment, realising NATO's risk sensitivities, it is likely to see a proactive strategy as an acceptable compromise.

Adopting a proactive strategy like persistent engagement within NATO's institutional structure will not, however, be easy. Interviews for this project revealed that NATO allies are unwilling to pool intelligence out of concern that they might then lose control over who has access to the shared information. A continual barrier to cooperation in the alliance is the tendency for states to keep certain "critical knowledge" to themselves.[22] Another issue is that currently allies are not even in agreement on the rules for engaging in unilateral offensive cyber operations, let alone multilateral initiatives.[23] In this sense, US Cyber Command is far ahead of European nations in the development of its proactive cyber posture, although there are signs that other nations are following suit – the UK for instance recently announced the launch of the offensively minded National Cyber Force.[24] As damaging cyber attacks grow in number, so too will the need to develop a coherent NATO strategy to manage their risk. Persistent engagement, well-suited to the identity of a risk community, is an obvious policy choice.

7.5 Recent developments and general trends

Since the research for this project was concluded, in December 2020, the United States discovered in its systems the Russian SolarWinds (or Sunburst) cyber campaign, a sophisticated espionage operation which targeted a number of US government departments.[25] Although this thesis was concerned with responses to instances of sabotage or subversion, the reaction of the United States to the campaign merits a short discussion here.

---

[20] Robin Emmott, 'NATO Cyber Command to Be Fully Operational in 2023', *Reuters*, 16 October 2018, https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9.
[21] Author interview with Toomas Hendrik Ilves, 25 March 2021.
[22] Author interview with Harri Tiido, 30 March 2021.
[23] Max Smeets, 'NATO Allies Need to Come to Terms With Offensive Cyber Operations', Lawfare, 14 October 2019, https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations.
[24] Conrad Prince, 'On the Offensive: The UK's New Cyber Force', RUSI, 23 November 2020, https://rusi.org/commentary/offensive-uk-new-cyber-force.
[25] The White House, 'FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government', The White House, 15 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

The response fell to the new administration of Joseph Biden.[26] In April 2021, the administration issued a series of penalties in response to SolarWinds and other "harmful foreign activities." These included formal attribution of SolarWinds to the Russian Foreign Intelligence Service (SVR), diplomatic sanctions, and economic sanctions – the latter in particular were seen by commentators as a more forceful response than past efforts to punish Russia.[27] This was because the sanctions package, in addition to imposing sanctions on individuals and companies that had aided Russian cyber operations, prohibited US financial institutions from purchasing Russian government bonds from the Russian Central Bank, the Russian National Wealth Fund, and the Russian Ministry of Finance.[28]

There are a number of important details that need to be examined before we can conclude that the Biden response represents a break with past punishments for cyber operations. Firstly, it appears that the sanctions targeting Russian sovereign debt were not explicitly linked to malicious cyber activities, but were rather intended as a larger political statement of a new administration towards Russia.[29] Secondly, while the package will undoubtedly generate effects that reach further than the more limited sanctions imposed under previous administrations, as Ellen Nakashima, a national security reporter at *The Washington Post*, explained: "[the sanctions imposed by the Biden administration] could be stronger still; they could sanction all sovereign debt, not just future issuances; they could do secondary markets, not just primary markets; they could also escalate sanctions to state-owned banks and energy companies and defence companies; put them on the designation list and put full blocking sanctions on them." She added that such measures "would really squeeze the [Russian] economy, but could also have spill-over effects, especially in Europe."[30] The last point is particularly important as it relates to the discussion of blowback in Chapter 3, which noted that although sanctions are a common choice for risk societies, which perceive them as less escalatory than other penalties (including cyber responses), these societies will be cognisant in their application of sanctions of their potential

[26] The outgoing Trump administration was at first reluctant to attribute the operation to Russia, but eventually formally indicated Russian culpability in January 2021. See: Dustin Volz, 'Trump Administration Says Russia Likely Behind Massive SolarWinds Hack', *Wall Street Journal*, 6 January 2021, sec. US, https://www.wsj.com/articles/white-house-removes-spokeswoman-at-agency-responding-to-solarwinds-hack-11609877635.

[27] The White House, 'FACT SHEET'; David E. Sanger and Andrew E. Kramer, 'U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation', *The New York Times*, 15 April 2021, sec. World, https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html.

[28] Office of Foreign Assets Control - U.S. Department of the Treasury, 'Directive 1 Under Executive Order of April 15, 2021 Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation', Department of the Treasury, 15 April 2021, https://home.treasury.gov/system/files/126/sovereign_debt_prohibition_directive_1.pdf; Ellen Nakashima, 'Biden Administration Imposes Significant Economic Sanctions on Russia over Cyberspying, Efforts to Influence Presidential Election', *The Washington Post*, 15 April 2021, https://www.washingtonpost.com/national-security/biden-to-announce-tough-sanctions-on-russia-over-cyber-spying/2021/04/15/a4c1d260-746e-11eb-948d-19472e683521_story.html.

[29] Robert Chesney, 'Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?', Lawfare, 15 April 2021, https://www.lawfareblog.com/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross.

[30] Ellen Nakashima in: The Hague Program for Cyber Norms, *Panel Discussion: Rethinking Cyber Espionage after the SolarWinds Hack* (YouTube, 2021), https://www.youtube.com/watch?v=fQjg1AOchBc.

unintended effects. In the case of the response to SolarWinds, the concern about the risk of blowback appears to have motivated the selection of more moderate sanctions.

Moreover, the response, much like decision-making in the wake of previous cyber incidents, was restrained by the perception of the risks of escalation. As President Biden himself put it when announcing the sanctions, "[t]he United States is not looking to kick off a *cycle of escalation* and conflict with Russia. We want a stable, *predictable* relationship [emphasis added]."[31] Thus, the Biden administration's response to SolarWinds, like responses to previous cyber incidents, appears to have been attentive to risk society fears of unpredictable future scenarios and reflexive concerns about the unintended effects the state's own actions.[32] The reaction to SolarWinds therefore indicates that cultural risk sensitivities are still shaping US responses to cyber operations, even under a new administration.

In terms of general future trends, what follows from this thesis is that we are likely to observe two contrasting pictures, depending on where we look. If we turn towards the Middle East, we are likely to see a continuation of intense cyber conflict, with possibilities for escalation. Iran is unlikely to abandon the use of cyber means in its security competition with Israel anytime soon – as we discussed in Chapter 3, the cyber operational environment empowers militarily weaker actors, meaning that cyber tools are particularly useful tool for Iran. Given Israel's culturally engrained impulse to punish foreign aggression, it too will not cease to engage in damaging and disruptive campaigns against its main adversary. The question is of course whether Israel will, over time, establish such a reputation for retaliation that Iran will start to moderate its cyber activity (for example, refrain from targeting critical infrastructure). There may be some possibility of this, although establishing a reputation will take time, meaning we will witness significant instability in Israeli-Iranian relations in at least the short and medium term.

If we turn to North America and Europe, the picture is different. The culturally rooted concerns about escalation will mean that such scenarios are less likely to materialise in relationships concerning risk societies. Indeed, as we saw, persistent engagement and defend forward have been designed with particular attention to minimising the risk of escalation. In setting out to intercept and neutralise hostile adversary cyber activity before it reaches US networks,[33] this strategy seeks to prevent situations that would require a response and therefore risk sparking tit-for-tat dynamics. Moreover, in operating continuously in adversary networks, the strategy increases US operatives' knowledge of these networks and helps tailor future offensive cyber operations to limit unintended effects and the potential for

[31] Biden quoted in: Sanger and Kramer, 'U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation'.
[32] It should also be noted here that the US response to SolarWinds raised questions regarding its appropriateness because, as far as is known at the time of writing, the operation was a targeted espionage campaign, the kind which the United States and the members of the Five Eyes Alliance likely engage in themselves. For a longer discussion of the possible motivations that shaped the response see: Chesney, 'Sanctioning Russia for SolarWinds'.
[33] U.S. Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', 2018, 4, https://bit.ly/2JcOwFr.

misinterpretation and escalation. While there may be other problems that arise from the use of proactive strategies (as Chapter 6 discussed, differences between NATO allies on the limits and bounds of offensive cyber operations could produce inter-allied tensions), escalation is unlikely to be one of them.

7.6 Avenues for further research

The findings of this thesis point to four areas that are particularly ripe for further research. First is the question of the cultural and historical roots of risk societies. Beck and the sociologists provided a detailed account of the process that leads to the development of risk societies, which they called reflexive modernisation, but the particular cultural values and beliefs that led some societies to become highly sensitive to risks, and others not, were underexplored. Scholars have since suggested that liberal states are likely to find it particularly difficult to cope with risks from technological development,[34] but this thesis showed that three liberal democracies reacted very differently to risk. While the empirical chapters provided an overview of the historical and cultural factors that contributed to the United States' and NATO's risk sensitivity, the analysis of this thesis focused mainly on the implications of risk society characteristics for responses to cyber attacks. These factors therefore remain for deeper analysis. Similarly, the thesis provided an explanation of the strategic cultural and historical determinants of threat society inclinations. This investigation too could be extended and deepened.

Secondly, future research could fruitfully apply the risk framework to new case studies. Research on the risk/ threat profiles of Russia, China, and Iran, all of which are particularly prolific offensive cyber operators in their rivalry with the countries discussed in this work, could enhance western understanding of adversaries' motives and limits in cyber conflict scenarios, thereby helping western nations avoid unwanted escalation resulting from their own cyber operations.

A third area that future scholars could address is how risk sensitivity manifests in the design and conduct of offensive cyber operations, as opposed to response decision-making (the subject of this thesis). In the war as risk management literature, for example, Coker argued that western risk societies sought to address the risks of going to war by making war more "humane" for both themselves and for those against whom they fight.[35] Much like the war as risk management literature explored how risk sensitivity changed the way in which western societies fight wars, the risk framework could also be applied to understand how different societies design and engage in operations of cyber sabotage. The concept of "consequence management" introduced in Chapter 3 could be extended to investigate how different states, according to their risk or threat identity, manage or fail to manage the consequences of their own offensive cyber operations in terms of collateral damage and other cascading effects. As an example, the highly precise Stuxnet operation, reportedly conducted by the United States and Israel to

[34] Adam Tooze, 'The Sociologist Who Could Save Us From Coronavirus', Foreign Policy, 1 August 2020, https://foreignpolicy.com/2020/08/01/the-sociologist-who-could-save-us-from-coronavirus/.
[35] Coker, *War in an Age of Risk*, 130.

hinder Iran's nuclear weapons programme, stands in stark contrast to the Russian NotPetya operation in 2017, which spread widely and indiscriminately around the world.[36] Given that Stuxnet was likely a joint operation between the United States and Israel, such research could also build on the findings of the Estonia case study, which showed that when a threat society is embedded in a risk community, it defers to the risk sensitivities of that community. Future research could ascertain whether Israel acts in a similar way when working in partnership with the United States.

Finally, further research is needed to determine the possible "exit" pathways from the risk society. Coker suggested that the "predisposition for risk-taking" by non-western societies "may focus us [western nations] to confront and overcome our own predisposition to be risk-averse."[37] A "dramatic event," "a more striking example of destruction [than even 9/11]" may, according to Coker, "take us beyond the risk age into something far different."[38] Beck, for his part, suggested that the process of "habituation" might mean that future generations in what are now risk societies don't share the same fears with today's generation.[39] Whether current risk societies are jolted out of their preoccupation with risks and back to a focus on threats by way of a seismic international event, or whether they simply "get used to" the diverse unintended side effects that technological development brings, remains to be seen. Deeper scholarly analysis of the cultural roots of the risk society will help answer this important question whose policy implications are potentially profound.

[36] Monica Kaminska, Fabio Cristiano, and Dennis Broeders, 'Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone', in *13th International Conference on Cyber Conflict: Going Viral*, ed. Tatiana Jančárková et al. (Tallinn, Estonia: NATO CCDCOE Publications, 2021).
[37] Coker, *War in an Age of Risk*, x.
[38] Coker, 176.
[39] Beck quoted in: Tooze, 'The Sociologist Who Could Save Us From Coronavirus'.

Bibliography

Aaviksoo, Jaak. ‘Meie Olemine Ja Kestmine’. In *Valik Riigikaitsealaseid Artikleid II*, 29–31. Tallinn, Estonia: Kaitseministeerium, 2008.

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford, California: Stanford University Press, 2010.

Adamsky, Dmitry (Dima). ‘From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force’. *Security Studies* 26, no. 1 (2 January 2017): 157–84.

———. ‘From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture’. *Journal of Strategic Studies* 41, no. 1–2 (23 February 2018): 33–60.

———. ‘The Israeli Odyssey toward Its National Cyber Security Strategy’. *The Washington Quarterly* 40, no. 2 (3 April 2017): 113–27.

Adler, Emanuel. ‘Seizing the Middle Ground: Constructivism in World Politics’. *European Journal of International Relations* 3, no. 3 (1 September 1997): 319–63.

Alden, Chris. *Foreign Policy Analysis: New Approaches*. Second edition. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2017.

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: Longman, 1999.

Alrifai, Oula A., Nakissa Jahanbani, and Mehdi Khalaji. ‘Iran’s Long Game in Syria’. The Washington Institute, 25 March 2021.

AP and TOI staff. ‘“Cyber Winter Is Coming,” Warns Israel Cyber Chief after Attack on Water Systems’. The Times of Israel, 28 May 2020.

Applegate, Scott. ‘Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare’. *Security & Privacy, IEEE* 9, no. 5 (2011): 16–22.

Apuzzo, Matt, and Sharon LaFraniere. ‘13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign’. *The New York Times*, 16 February 2018.

Asmus, Ronald D., and Robert C. Nurick. ‘NATO Enlargement and the Baltic States’. *Survival* 38, no. 2 (1 June 1996): 121–42.

Associated Press. ‘Anonymous Hacker Attack on Israeli Websites “Causes Little Real Damage”’. The Guardian, 8 April 2013.

Avant, Deborah D. ‘Are the Reluctant Warriors out of Control? Why the U.S. Military Is Averse to Responding to Post-cold War Low-level Threats’. *Security Studies* 6, no. 2 (December 1996): 51–90.

Ayyub, Rami. ‘Israel Says It Thwarted Foreign Cyber Attack on Defence Industry’. *Reuters*, 12 August 2020.

Azodi, Sina. ‘Israel’s “Shadow” War with Iran Risks Playing out in the Open’. *Atlantic Council* (blog), 16 April 2021.

Bachner, Michael, and TOI Staff. ‘By Design, Cyberattack on Iran Port Caused Only Minor Damage – Report’. The Times of Israel, 20 May 2020.

Baker, Peter. ‘How Trump’s Election Shook Obama: “What If We Were Wrong?”’ *The New York Times*. Accessed 20 April 2020.

Banks, William. ‘State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0 Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations’. *Texas Law Review* 95, no. 7 (2017): 1487–1514.

Barnes, Julian E. ‘U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections’. *The New York Times*, 23 October 2018.

———. ‘U.S. Cyberforce Was Deployed to Estonia to Hunt for Russian Hackers’. *The New York Times*, 3 December 2020.

Barnett, Michael N. ‘Identity and Alliances in the Middle East’. In *The Culture of National Security*, edited by Peter J. Katzenstein. New York: Columbia University Press, 1996.

Bar-Tal, Daniel, and Dikla Antebi. ‘Siege Mentality in Israel’. *International Journal of Intercultural Relations* 16, no. 3 (1 June 1992): 251–75.

BBC News. ‘US Sanctions North Korea over Sony’. *BBC News*, 3 January 2015.
BBC News, ‘Cyber-Attack: US and UK Blame North Korea for WannaCry’, *BBC News*, 19 December 2017.
Beck, Ulrich. *Risk Society: Towards a New Modernity*. London: SAGE, 1992.
———. ‘The Reinvention of Politics: Towards a Theory of Reflexive Modernization’. In *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, edited by Ulrich Beck, Anthony Giddens, and Scott Lash. Cambridge: Polity Press, 1994.
———. ‘The Silence of Words: On Terror and War’. *Security Dialogue* 34, no. 3 (1 September 2003): 255–67. https://doi.org/10.1177/09670106030343002.
———. ‘The Terrorist Threat: World Risk Society Revisited’. *Theory, Culture & Society* 19, no. 4 (1 August 2002): 39–55. https://doi.org/10.1177/0263276402019004003.
———. *World Risk Society*. Cambridge: Polity, 1999.
Beck, Ulrich, Anthony Giddens, and Scott Lash. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge: Polity in association with Blackwell, 1994.
Beehner, Lionel. ‘Israel and the Doctrine of Proportionality’. *Council on Foreign Relations* (blog), 13 July 2006.
Bellovin, Steven M., Susan Landau, and Herbert S. Lin. ‘Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications’. *Journal of Cybersecurity* 3, no. 1 (2017): 59–68.
Berger, Joseph. ‘A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case’. *The New York Times*, 25 March 2016.
Berger, Thomas U. ‘Norms, Identity, and National Security in Germany and Japan’. In *The Culture of National Security*, 317–56. New York: Columbia University Press, 1996.
Bergman, Ronen, and David M. Halbfinger. ‘Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks’. *The New York Times*, 20 May 2020.
Berman, Lazar. ‘Iran Showing Increasing Nerve as Fight with Israel Spreads to the Sea’. The Times of Israel, 26 March 2021.
Bertelsmann Foundation. ‘Episode 1 Russian Cyber-Attack on Estonia’. Bertelsmann Foundation, 4 February 2021.
Betts, Richard K. ‘Striking First: A History of Thankfully Lost Opportunities’. *Ethics & International Affairs* 17, no. 1 (March 2003): 17–24.
Biddle, Sam. ‘Anonymous Is Losing Its War Against Israel’. Gizmodo, 19 November 2012.
Bjola, Corneliu, and Markus Kornprobst. ‘Security Communities and the Habitus of Restraint: Germany and the United States on Iraq’. *Review of International Studies* 33, no. 2 (April 2007): 285–305.
Blake, Aaron. ‘Analysis | NSA Director Mike Rogers’s Remarkable Comments about Trump’s Russia Efforts — or Lack Thereof’. *Washington Post*, 28 February 2018.
Blanchard, B. Wayne. ‘Guide to Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation: A Tutorial on Emergency Management, Broadly Defined, Past and Present’. FEMA Emergency Management Institute, 22 October 2008.
Blomfield, Adrian. ‘Russia Accused over Estonian “Cyber-Terrorism”’. The Telegraph, 17 May 2007.
Bodeau, Deborah, and Richard Graubart. ‘Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment’. MTR130432. MITRE Technical Report. Bedford, MA: The MITRE Corporation, November 2013.
Booth, Ken. ‘The Concept of Strategic Culture Affirmed’. In *Strategic Power: USA/USSR*, edited by C. G. Jacobsen, David R. Jones, Bill Kincade, and Ken Booth. Basingstoke: Macmillan, 1990.
Borghard, Erica. ‘Economic Sanctions Should Not Always Be the Go-to Foreign Policy Tool’. Washington, D.C.: Atlantic Council, 22 February 2021.
Borghard, Erica D., and Shawn W. Lonergan. ‘Cyber Operations as Imperfect Tools of Escalation’. *Strategic Studies Quarterly*, Fall 2019: 122-145.
Borghard, Erica D., and Shawn W. Lonergan. ‘Why Are There No Cyber Arms Control Agreements?’ *Council on Foreign Relations Net Politics* (blog), 16 January 2018.

Broeders, Dennis, Liisi Adamson, and Rogier Creemers, 'A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' (The Hague: The Hague Program for Cyber Norms, 2019).
Browne, Ryan. 'McMaster: "We Have Failed to Impose Sufficient Costs" on Russia'. CNN, 4 April 2018.
Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*. London: Hurst & Company, 2016.
———. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.
Buchanan, Ben, and Fiona Cunningham. 'Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis' 3, no. 4 (Fall 2020): PDF not yet available.
Carson, Austin. 'Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War'. *International Organization* 70, no. 1 (ed 2016): 103–31.
———. *Secret Wars: Covert Conflict in International Politics*. Princeton, New Jersey: Princeton University Press, 2018.
Carson, Austin, and Keren Yarhi-Milo. 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret'. *Security Studies* 26, no. 1 (2 January 2017): 124–56.
Center for Strategic & International Studies (CSIS). *10 Years of Cyber Estonia: What Will the Next Decade Bring?* Washington, D.C.: Center for Strategic & International Studies, 2017.
Checkel, Jeffrey T. 'The Constructivist Turn in International Relations Theory'. *World Politics* 50, no. 2 (1998): 324–48.
Chesney, Robert. 'Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?' Lawfare, 15 April 2021.
Cisco Systems. 'Remotely Triggered Black Hole Filtering— Destination Based and Source Based'. Cisco, 2005.
Clapper, James R. *Facts and Fears: Hard Truths from a Life in Intelligence*. New York: Penguin Random House Large Print, 2018.
Clapton, William. 'Risk in International Relations'. *International Relations* 25, no. 3 (2011): 280–95.
Clark, D. 'The Design Philosophy of the DARPA Internet Protocols'. *ACM SIGCOMM Computer Communication Review* 18, no. 4 (1 August 1988): 106–14.
Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st ed. New York: Ecco, 2010.
Clemente, Dave. *Cyber Security and Global Interdependence What Is Critical?* London: Chatham House, 2013.
CNBC. 'US Accuses China of Violating Bilateral Anti-Hacking Agreement'. CNBC, 9 November 2018.
Coker, Christopher. 'Between Iraq and a Hard Place'. *The RUSI Journal* 151, no. 5 (1 October 2006): 14–19.
———. *Globalisation and Insecurity in the Twenty-First Century: NATO and the Management of Risk*. Adelphi Papers ; No. 345. Oxford and New York: Oxford University Press for the International Institute for Strategic Studies, 2002.
———. *Humane Warfare*. London ; New York: Routledge, 2001.
———. *Waging War without Warriors?: The Changing Culture of Military Conflict*. Boulder, Co. ; London: Lynne Rienner Publishers, 2002.
———. *War in an Age of Risk*. Cambridge: Polity Press, 2009.
Cormac, Rory, and Richard J. Aldrich. 'Grey Is the New Black: Covert Action and Implausible Deniability'. *International Affairs* 94, no. 3 (1 May 2018): 477–94.
Corn, Gary, and Eric Talbot Jensen. 'The Use of Force and Cyber Countermeasures'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 4 June 2018.
Council on Foreign Relations. 'Estonian Denial of Service Incident'. Council on Foreign Relations, May 2007.
Council on Foreign Relations. 'A Conversation with Benjamin Netanyahu'. Council on Foreign Relations, 8 July 2010.
Crossley, Gabriel, and Katya Golubkova. 'Explainer-China, Russia Vulnerable to Dollar Risks as Sanctions from West Multiply'. *Reuters*, 23 March 2021.

Daniel, Michael. ‘Our Latest Tool to Combat Cyber Attacks: What You Need to Know’. The White House, 1 April 2015.
Davis, Joshua. ‘Hackers Take Down the Most Wired Country in Europe’. *Wired*, 21 August 2007.
Deibert, Ronald J. ‘Bounding Cyber Power: Escalation and Restraint in Global Cyberspace’. In *Organized Chaos: Reimagining the Internet*, edited by Mark Raymond and Gordon Smith. Ontario, Canada: Centre for International Governance Innovation, 2014.
Deibert, Ronald J., and Rafal Rohozinski. ‘Risking Security: Policies and Paradoxes of Cyberspace Security’. *International Political Sociology* 4, no. 1 (2010): 15–32.
Department of Defense. ‘Department of Defense – Defense Science Board Task Force on Cyber Deterrence’. Washington, D.C.: Department of Defense, 2017.
———. ‘Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934’. Washington, D.C.: Department of Defense, November 2011.
———. ‘Summary: Department of Defense Cyber Strategy’. Washington, D.C.: Department of Defense, 2018.
Department of Justice. ‘Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities’. Washington, D.C.: United States Department of Justice, 24 March 2016.
Desch, Michael C. ‘Culture Clash: Assessing the Importance of Ideas in Security Studies’. *International Security* 23, no. 1 (1 July 1998): 141–70.
DeYoung, Karen, Shira Rubin, and Kareem Fahim. ‘U.S. Prepares for Further Talks with Iran as Tehran Blames Israel for Attack on Nuclear Facility’. *Washington Post*, 13 April 2021.
Doffman, Zak. ‘Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First’. Forbes, 6 May 2019.
Dostri, Omer. ‘Cyber-Warfare between Iran and Israel’. JISS, 3 June 2020.
Douglas, Mary, and Aaron B. Wildavsky. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley: University of California Press, 1982.
Doyle, Michael W. ‘Striking First’. In *Striking First: Preemption and Prevention in International Conflict*, edited by Stephen Macedo. University Center for Human Values Series. Princeton, NJ: Princeton University Press, 2008.
Duffield, John S., Theo Farrell, Richard Price, and Michael C. Desch. ‘Isms and Schisms: Culturalism versus Realism in Security Studies’. *International Security* 24, no. 1 (1999): 156–80.
Dupont, Benoît. ‘The Cyber-Resilience of Financial Institutions: Significance and Applicability’. *Journal of Cybersecurity* 5, no. 1 (1 January 2019): 1–17.
Economist Intelligence Unit and Booz Allen Hamilton. ‘Cyber Power Index’. Booz Allen Hamilton, 2011.
Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod. ‘Strategic Aspects of Cyberattack, Attribution, and Blame’. *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (2017): 2825–30.
Egloff, Florian J. ‘Contested Public Attributions of Cyber Incidents and the Role of Academia’. *Contemporary Security Policy* 41, no. 1 (2 January 2020): 55–81.
———. ‘Public Attribution of Cyber Intrusions’. *Journal of Cybersecurity* 6, no. 1 (1 January 2020).
Eiran, Ehud, and Martin B. Malin. ‘The Sum of All Fears: Israel’s Perception of a Nuclear-Armed Iran’. *The Washington Quarterly* 36, no. 3 (1 August 2013): 77–89.
Eisenkot, Gadi, and Gabi Siboni. ‘The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran’s Malign Regional Influence’. The Washington Institute, 4 September 2019.
Elliott, Anthony. ‘Beck’s Sociology of Risk: A Critical Assessment’. *Sociology* 36, no. 2 (1 May 2002): 293–315.
Emmott, Robin. ‘NATO Cyber Command to Be Fully Operational in 2023’. *Reuters*, 16 October 2018.
ENISA. ‘Communication Network Dependencies for ICS/SCADA Systems’. Report/Study, December 2016.
ERR News. ‘Estonia and US Joint Operation Strengthens Cyber Defense’. ERR.ee, 4 December 2020.

Estes, Adam Clark. ‘Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back’. The Atlantic, 8 April 2013.
Estonian Foreign Intelligence Service. ‘International Security and Estonia’. Estonian Foreign Intelligence Service Välisluureamet, 2018.
———. ‘International Security and Estonia’. Estonian Foreign Intelligence Service Välisluureamet, 2019.
———. ‘International Security and Estonia’. Estonian Foreign Intelligence Service Välisluureamet, 2020.
———. ‘International Security and Estonia’. Estonian Foreign Intelligence Service Välisluureamet, 2021.
Estonian Information Board. ‘International Security and Estonia’. Estonian Information Board Teabeamet, 2016.
———. ‘International Security and Estonia’. Estonian Information Board Teabeamet, 2017.
European Commission. ‘Annual Work Programme 2010: Prevention, Preparednesss and Consequence Management of Terrorism and Other Security Related Risks’. European Commission, 2010.
European Commission, Environment Directorate-General, Bristol University of the West of England, and Science Communication Unit. ‘The Precautionary Principle: Decision-Making under Uncertainty.’ Science for Environment Policy. Brussels, Belgium: European Commission, September 2017.
FBI. ‘Iranians Charged with Hacking U.S. Financial Sector’. Story. Federal Bureau of Investigation, 24 March 2016.
Fearon, James D. ‘Rationalist Explanations for War’. *International Organization* 49, no. 3 (1995): 379–414.
Feifer, Gregory. ‘Estonia Seeks Stronger EU Response To Russia’. NPR.org, 9 September 2008.
Finnemore, Martha. *National Interests in International Society*. Cornell Studies in Political Economy. Ithaca, NY: Cornell University Press, 2017.
Finnemore, Martha, and Kathryn Sikkink. ‘International Norm Dynamics and Political Change’. *International Organization* 52, no. 4 (1998): 887–917.
Finnemore, Martha, and Duncan B. Hollis, ‘Constructing Norms for Global Cybersecurity’, *American Journal of International Law* 110, no. 3 (July 2016): 425–79.
Fischerkeller, Michael P. ‘The Structural and Strategic Imperative: The Need for Persistent Engagement’. Washington, D.C.: IDA Institute for Defense Analyses, October 2018.
Fischerkeller, Michael P., and Richard J. Harknett. ‘Deterrence Is Not a Credible Strategy for Cyberspace’. *Orbis* 61, no. 3 (2017): 381–93.
———. ‘Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation’. *The Cyber Defense Review*, 2019, 267–87.
———. ‘Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect’. Lawfare, 6 February 2020.
NBC News. ‘Flashback: President Bush on Putin’s “Soul”’, 27 March 2014.
Foreign and Commonwealth Office. ‘Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks’. gov.uk, 19 December 2017.
Francis, David. ‘Obama Slams North Korea With Sanctions for Sony Hack’. *Foreign Policy* (blog), 2 January 2015.
Freedberg Jr., Sydney J. ‘A “Solarium” For Hacking: Sen. King Launches Cyber Strategy Panel’. Breaking Defense, 13 May 2019.
Frei, Jasper. ‘Israel’s National Cybersecurity and Cyberdefense Posture: Policy and Organizations’. Application/pdf. Zürich: ETH Zurich, September 2020.
Freilich, Charles. ‘Israel’s National Security Policy’. In *The Oxford Handbook of Israeli Politics and Society*, edited by Hazan Reuven, Dowty Alan, Hofnung Menachen, and Rahat Gideon. Oxford: Oxford University Press, 2021.
Furedi, Frank. ‘Precautionary Culture and the Rise of Possibilistic Risk Assessment’. *Erasmus Law Review* 2, no. 2 (November 2009): 197–220.
Garrett, Nathan G. ‘NATO, Security and Risk Management: From Kosovo to Kandahar, by Williams, M. J.’ *The Journal of Slavic Military Studies* 23, no. 3 (3 September 2010): 525–27.

Gerecht, Reuel Marc, and Ray Takeyh. ‘Iran’s Holocaust Denial Is Part of a Malevolent Strategy’. *Washington Post*, 27 May 2016.
Gerring, John. *Case Study Research: Principles and Practices*. Cambridge, UK: Cambridge University Press, 2016.
Gheciu, Alexandra. ‘Security Institutions as Agents of Socialization? NATO and the “New Europe”’. *International Organization* 59, no. 4 (2005): 973–1012.
Giddens, Anthony. ‘Risk Society: The Context of British Politics’. In *The Politics of Risk Society*, edited by Jane Franklin. Cambridge: Polity Press, 1998.
Giegerich, Bastian. *European Security and Strategic Culture*. Baden-Baden: Nomos, 2006.
Glenn, John, and Darryl Howlett. ‘Neorealism’. In *Neorealism versus Strategic Culture*, edited by John Glenn, Darryl A. Howlett, and Stuart Poore. Critical Security Series. Abingdon, Oxon ; New York, NY: Routledge, 2018.
Gold, Josh. ‘How Estonia Uses Cybersecurity to Strengthen Its Position in NATO’. ICDS, 27 May 2019.
Goldenberg, Ilan, Nicholas A. Heras, Kaleigh Thomas, and Jennie Matuschak. ‘Countering Iran in the Gray Zone What the United States Should Learn from Israel’s Operations in Syria’. Countering Iran in the Gray Zone. Center for a New American Security, 2020.
Goldman, Emily. ‘From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy’. *Texas National Security Review* 3, no. 4 (Fall 2020): 84–101.
Goldsmith, Jack. ‘The Puzzle of the GRU Indictment’. Lawfare, 21 October 2020.
Goldsmith, Jack, and Stuart Russell. ‘Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations’. Stanford, CA: Hoover Working Group on National Security, Technology, and Law, 5 June 2018.
Goldsmith, Jack, and Robert D. Williams. ‘The Failure of the United States’ Chinese-Hacking Indictment Strategy’. Lawfare, 28 December 2018.
Goldstein, Judith, and Robert O. Keohane. *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*. Ithaca: Cornell University Press, 1993.
Gompert, David C., and Hans Binnendijk. ‘The Power to Coerce: Countering Adversaries Without Going to War’. Santa Monica, CA: RAND Corporation, 3 March 2016.
Goodman, Will. ‘Cyber Deterrence: Tougher in Theory than in Practice?’ *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–35.
Götz, Elias. ‘Enemy at the Gates: A Neoclassical Realist Explanation of Russia’s Baltic Policy’. *Foreign Policy Analysis* 15, no. 1 (1 January 2019): 99–117.
Government of the Republic of Estonia. ‘Declaration of the Minister of Foreign Affairs of the Republic of Estonia’. Government Office, 1 May 2007.
Gray, Colin S. ‘Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?’ Carlisle, PA: Strategic Studies Institute, US Army War College, 2006.
———. *National Security Dilemmas: Challenges and Opportunities*. 1st ed. Book Collections on Project MUSE. Washington, D.C.: Potomac Books, 2009.
———. ‘National Style in Strategy: The American Example’. *International Security* 6, no. 2 (1981): 21–47.
———. ‘Out of the Wilderness: Prime Time for Strategic Culture’. *Comparative Strategy* 26, no. 1 (8 May 2007): 1–20.
Greenberg, Andy. ‘How the Worst Cyberattack in History Hit American Hospitals’. Slate Magazine, 5 November 2019.
———. ‘OPM Now Admits 5.6m Feds’ Fingerprints Were Stolen By Hackers’. *Wired*, 23 September 2015.
———. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. New York: Doubleday, 2019.
———. ‘The Untold Story of NotPetya, The Most Devastating Cyberattack in History’. *Wired Magazine*, 22 August 2018.
Groll, Elias. ‘Security Firms Tie WannaCry Ransomware to North Korea’. *Foreign Policy* (blog). Accessed 31 March 2020.
Gross, Judah Ari. ‘IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle’. The Times of Israel, 5 May 2019.

Gross Stein, Janice. ‘Decision Making: Rational, Psychological, and Neurological Models’. In *Foreign Policy Theories Actors Cases*, edited by Steve Smith, Amelia Hadfield, and Tim Dunne. Oxford: Oxford University Press, 2012.
Gunter, Aleksei. ‘Estonia, Russia Expel Diplomats’. The Baltic Times, 25 March 2004.
Gur, Haviv Rettig. ‘“Anonymous” Escalates Cyber-War against Israel and pro-Israel Groups’. The Times of Israel, 16 November 2012.
Hameiri, Shahar, and Florian P. Kühn. ‘Introduction: Risk, Risk Management and International Relations’. *International Relations* 25, no. 3 (2011): 275–79.
Handel, Michael I. ‘The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security’. In *The Making of Strategy: Rulers, States, and War*, edited by Williamson Murray, Macgregor Knox, and Alvin Bernstein. Cambridge, UK: Cambridge University Press, 1994.
Harknett, Richard J. ‘Progress Is the Promise in National Cybersecurity Strategy’. Lawfare, 23 March 2020.
———. ‘The Logic of Conventional Deterrence and the End of the Cold War’. *Security Studies* 4, no. 1 (September 1994): 86–114.
———. ‘United States Cyber Command’s New Vision: What It Entails and Why It Matters’. Lawfare, 23 March 2018.
Harknett, Richard J., and Emily Goldman. ‘The Search for Cyber Fundamentals’. *Journal of Information Warfare* 15, no. 2 (2016): 81–88.
Harknett, Richard J., and Joseph S. Nye. ‘Correspondence: Is Deterrence Possible in Cyberspace?’ *International Security* 42, no. 2 (November 2017): 196–99.
Harknett, Richard J., and Max Smeets. ‘Cyber Campaigns and Strategic Outcomes’. *Journal of Strategic Studies*, 4 March 2020, 1–34.
Healey, Jason. ‘The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 15 June 2016.
———. ‘The Implications of Persistent (and Permanent) Engagement in Cyberspace’. *Journal of Cybersecurity* 5, no. 1 (1 January 2019).
Heinegg, Wolff Heintschel von. ‘Proportionality and Collateral Damage’. In *Max Planck Encyclopedia of Public International Law [MPEPIL]*, October 2015.
Heller, Nathan. ‘Estonia, the Digital Republic’. *The New Yorker*, 11 December 2017.
Heng, Yee-Kuang. ‘The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions’. *Contemporary Security Policy* 39, no. 4 (2 October 2018): 544–58.
———. ‘War as Risk Management’. London School of Economics and Political Science, 2003.
———. *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*. Contemporary Security Studies. London; New York: Routledge, 2006.
Herman, Robert G. ‘Identity, Norms, and National Security’. In *The Culture of National Security*, edited by Peter J. Katzenstein, 271–316. New York: Columbia University Press, 1996.
Herzog, Stephen. ‘Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses’. *Journal of Strategic Security* 4, no. 2 (2011): 49–60.
Hills, Mils. ‘Hybrid Threats A Strategic Communications Perspective: 2007 Cyber Attacks on Estonia’. In *Hybrid Threats: A Strategic Communications Perspective Annex of Case Studies*, edited by Benjamin Heap. Riga, Latvia: NATO Stratcom Centre of Excellence, 2019.
Hinck, Garrett, and Tim Maurer. ‘Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity’. *Journal of National Security Law and Policy* 10, no. 3 (January 2020): 525–61.
Hirschfeld Davis, Julie, and David E. Sanger. ‘Obama Says U.S. Will Retaliate for Russia’s Election Meddling’. *The New York Times*, 15 December 2016.
Hodgson, Quentin, Logan Ma, Krystyna Marcinek, and Karen Schwindt. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*. Santa Monica, CA: RAND Corporation, 2019.
Ikenberry, G. John. ‘The Illusion of Geopolitics: The Enduring Power of the Liberal Order Essay’. *Foreign Affairs* 93, no. 3 (2014): [i]-91.

Ilves, Toomas Hendrik. ‘A Digital Defense Alliance’. *Berlin Policy Journal* (blog), 10 January 2018.
International Telecommunications Union. ‘Global Cybersecurity Index (GCI) 2018’. Geneva, Switzerland: International Telecommunications Union, 2019.
Isikoff, Michael. ‘Ex-Sanctions Czar Bashes Obama Administration’s “weak” Response to Russian Interference’. Yahoo News, 20 April 2018.
Isikoff, Michael, and David Corn. *Russian Roulette: The Inside Story of Putin’s War on America and the Election of Donald Trump*. New York: Hachette Book Group, Inc., 2018.
Israel Defense Forces (IDF). ‘CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets.’ Twitter, 5 May 2019.
Israel Defense Forces (transl. Belfer Center for Science and International Affairs). ‘Deterring Terror How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israel Defense Forces’. Harvard Kennedy School, August 2016.
Israel Ministry of Foreign Affairs. ‘PM Netanyahu Addresses UN General Assembly 1 Oct 2013’. Israel Ministry of Foreign Affairs, 1 October 2013.
Israeli, Zipi. ‘National Security Index Public Opinion Study 2019-2020’. INSS, 2020.
e-Estonia. ‘I-Voting’. Accessed 4 March 2019.
Jacobsen, Jeppe T. ‘Cyber Offense in NATO: Challenges and Opportunities’. *International Affairs* 00, no. 0 (31 March 2021): 1–18.
Jarvis, Darryl S. L. ‘Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis’. *Global Society* 21, no. 1 (2007): 23–46.
Jarvis, Darryl S. L., and Martin Griffiths. ‘Learning to Fly: The Evolution of Political Risk Analysis’. *Global Society* 21, no. 1 (2007): 5–21.
Jarvis, Darryl S.L., and Martin Griffiths. ‘Risk and International Relations: A New Research Agenda?’ *Global Society* 21, no. 1 (1 January 2007): 1–4.
Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman & Littlefield, 2017.
Jerusalem Post Staff. ‘Hamas Cyber-Attack Thwarted by Israel Security Forces’. The Jerusalem Post, 5 May 2019.
Jervis, Robert. ‘Cooperation under the Security Dilemma’. *World Politics* 30, no. 2 (1978): 167–214.
Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, New Jersey: Princeton University Press, 1976.
———. ‘Pinker the Prophet’. Edited by Steven Pinker. *The National Interest*, no. 116 (December 2011): 54–64.
Johnson, Dominic D. P. *Strategic Instincts: The Adaptive Advantages of Cognitive Biases in International Politics*. Princeton, N.J.; Oxford: Princeton University Press, 2020.
Johnson, Dominic D. P., Daniel T. Blumstein, James H. Fowler, and Martie G. Haselton. ‘The Evolution of Error: Error Management, Cognitive Constraints, and Adaptive Decision-Making Biases’. *Trends in Ecology & Evolution* 28, no. 8 (August 2013): 474–81.
Johnson, Dominic D.P., and Dominic Tierney. ‘Bad World: The Negativity Bias in International Politics’. *International Security* 43, no. 3 (1 February 2019): 96–140.
Johnston, Alastair Iain. ‘Thinking about Strategic Culture’. *International Security* 19, no. 4 (1995): 32–64.
Jones, James. ‘Putin’s Youth Movement Provides a Sinister Backdrop to Russia’s Protests | James Jones’. *The Guardian*, 8 December 2011, sec. Opinion.
Joseph S. Nye, Jr. ‘From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?’ *Bulletin of the Atomic Scientists* 69, no. 5 (2013): 8–14.
Joye, Christopher. ‘Interview Transcript: Former Head of the NSA and Commander of the US Cyber Command, General Keith Alexander’. Australian Financial Review, 7 May 2014.
Kahneman, Daniel, and Amos Tversky. ‘Prospect Theory: An Analysis of Decision under Risk’. *Econometrica* 47, no. 2 (1979): 263–91.
Kaitsepolitseiamet. ‘Security Police of the Republic of Estonia Annual Review 2006’. Kaitsepolitseiamet, 2006.
———. ‘Security Police of the Republic of Estonia Annual Review 2007’. Kaitsepolitseiamet, 2007.
Kaminska, Monica, Fabio Cristiano, and Dennis Broeders, ‘Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone’, in *13th*

International Conference on Cyber Conflict: Going Viral, ed. Tatiana Jančárková et al. (Tallinn, Estonia: NATO CCDCOE Publications, 2021).
Kaminska, Monica. 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks'. *Journal of Cybersecurity* 7, no. 1 (9 March 2021).
———. 'Risk Aversion Is at the Heart of the Cyber Response Dilemma'. *Council on Foreign Relations Net Politics* (blog), 31 March 2021.
Karp, Brad S. 'Federal Guidance on the Cybersecurity Information Sharing Act of 2015'. Harvard Law School Forum on Corporate Governance, 3 March 2016.
Kaska, Kadri, Anna-Maria Talihärm, and Eneken Tikk. 'Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007'. In *International Cyber Security : Legal & Policy Proceedings 2010*, 40−66. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2007.
Katzenstein, Peter J. 'Introduction: Alternative Perspectives on National Security'. In *The Culture of National Security*, edited by Peter J. Katzenstein, 1–32. New York: Columbia University Press, 1996.
———, ed. *The Culture of National Security*. New York: Columbia University Press, 1996.
Kaye, Dalia Dassa, Alireza Nader, and Parisa Roshan. *Israel and Iran: A Dangerous Rivalry*. Santa Monica, CA: RAND National Defense Research Institute, 2011.
Kello, Lucas. 'Les Cyberarmes : Dilemmes et Futurs Possibles'. *Politique Étrangère* 4 (Winter 2014): 139–50.
———. 'The Advantages of Latitude: Estonia's Post-Communist Success Story'. In *Democratization and Security in Central and Eastern Europe and the Post-Soviet States*, edited by David Bosold, Petr Drulák, and Nik Hynek. Baden-Baden: Nomos, 2012.
———. 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft'. *International Security* 38, no. 2 (2013): 7–40.
———. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.
Kennan, George F. 'Opinion: A Fateful Error'. *The New York Times*, 5 February 1997.
Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. First Princeton Classic Edition. Princeton; Oxford: Princeton University Press, 2005.
———. 'International Institutions: Can Interdependence Work?' *Foreign Policy*, no. 110 (1998): 82–194.
Keohane, Robert O., and Lisa L. Martin. 'The Promise of Institutionalist Theory'. *International Security* 20, no. 1 (1995): 39–51.
Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. 4th ed. Boston ; London: Longman, 2012.
Keohane, Robert O., and Joseph S. Nye Jr. 'Power and Interdependence'. *Survival* 15, no. 4 (1 July 1973): 158–65.
Kershner, Isabel. 'Iran Fires Rockets Into Golan Heights From Syria, Israelis Say'. *The New York Times*, 9 May 2018.
Khazan, Olga. 'Anonymous Is Hacking Israeli Web Sites'. *Washington Post*, 17 November 2012.
Kier, Elizabeth. 'Culture and French Military Doctrine Before World War II'. In *The Culture of National Security*, edited by Peter J. Katzenstein, 186–215. New York: Columbia University Press, 1996.
King, Angus, and Mike Gallagher, eds. 'United States of America Cyberspace Solarium Commission', March 2020.
King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press, 1994.
Kingsley, Patrick, David E. Sanger, and Farnaz Fassihi. 'After Nuclear Site Blackout, Thunder From Iran, and Silence From U.S.' *The New York Times*, 12 April 2021.
Kirch, Marika, and Aksel Kirch. 'Search for Security in Estonia: New Identity Architecture'. *Security Dialogue* 26, no. 4 (1 December 1995): 439–48.
Koerner, Brendan I. 'Inside the OPM Hack, the Cyberattack That Shocked the US Government'. *Wired*, 23 October 2016.
Kohler, Kevin. 'Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations'. ETH Zurich, 2020.

Kostyuk, Nadiya, Scott Powell, and Matt Skach. 'Determinants of the Cyber Escalation Ladder'. *The Cyber Defense Review* 3, no. 1 (2018): 123–34.
Kotka, Taavi, and Innar Liiv. 'Concept of Estonian Government Cloud and Data Embassies'. In *Electronic Government and the Information Systems Perspective*, edited by Andrea Kő and Enrico Francesconi, 9265:149–62. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015.
Kotzanikolaou, Panayiotis, Marianthi Theoharidou, and Dimitris Gritzalis. 'Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects'. In *Critical Information Infrastructure Security*, edited by Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, and Stephen Wolthusen, 104–15. Lecture Notes in Computer Science. Berlin and Heidelberg: Springer, 2013.
Kreps, Sarah, and Jacquelyn Schneider. 'Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics'. *Journal of Cybersecurity* 5, no. 1 (1 January 2019).
Kubovič, Ondrej. 'EternalBlue Reaching New Heights since WannaCryptor Outbreak'. WeLiveSecurity, 17 May 2019.
Kwai, Isabella. 'Australian Parliament Reports Cyberattack on Its Computer Network'. *The New York Times*, 7 February 2019.
Landler, Mark, and John Markoff. 'Digital Fears Emerge After Data Siege in Estonia'. *The New York Times*, 29 May 2007.
Langner, Ralph. 'To Kill A Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve'. *The Langner Group*, November 2013, 37.
Lauristin, Marju, Peeter Vihalemm, and Karl Erik Rosengren. *Return to the Western World: Cultural and Political Perspectives on the Estonian Post-Communist Transition*. Tartu, Estonia: Tartu University Press, 1997.
Levs, Josh. 'Iran Leader's Call to "annihilate" Israel Sparks Fury'. CNN, 10 November 2014.
Libicki, Martin C. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation, 2012.
———. 'Expectations of Cyber Deterrence'. *Strategic Studies Quarterly* 12, no. 4 (2018): 44–57.
Lin, Herbert. 'Attribution of Malicious Cyber Incidents: From Soup to Nuts'. *The Cyber Issue*, Winter 2016.
———. 'Escalation Dynamics and Conflict Termination in Cyberspace'. *Strategic Studies Quarterly* 6, no. 3 (2012): 46–70.
Lindsay, Jon R. 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack'. *Journal of Cybersecurity* 1, no. 1 (27 November 2015): 53–67.
Little, Richard G. 'Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures'. *Journal of Urban Technology* 9, no. 1 (April 2002): 109–23.
Lorents, Peeter, Rain Ottis, and Raul Rikk. 'Cyber Society and Cooperative Cyber Defence'. In *Internationalization, Design and Global Development*, edited by Nuray Aykin, 180–86. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009.
Loukianov, Fiodor. 'Russia, a Revisionist Power?' *Politique Étrangère* 80, no. 2 (Summer 2015).
Luik, Jüri. 'Estonia's Long Road to NATO'. *ICDS* (blog), 22 April 2019.
Lupton, Deborah. 'Sociology and Risk'. In *Beyond the Risk Society: Critical Reflections on Risk and Human Security*, edited by Gabe Mythen and Sandra Walklate. Maidenhead, Berkshire: Open University Press, 2006.
Lynn III, William, J. 'Defending a New Domain: The Pentagon's Cyberstrategy'. *Foreign Affairs* 89, no. 5 (October 2010): 97–108.
Männik, Erik. 'Small States: Invited to NATO — Able to Contribute?' *Defense & Security Analysis* 20, no. 1 (January 2004): 21–37.
Mardiste, David. 'Show Putin Strength, Not Weakness, Says Estonian Defense Minister'. *Atlantic Council* (blog), 10 November 2014.
Maschmeyer, Lennart. 'Persistent Engagement Neglects Secrecy at Its Peril'. Lawfare, 4 March 2020.
Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan. 'A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy'. *Georgetown Journal of International Affairs* 17, no. 3 (2016): 77–84.

Maylam, Joelle Garriaud. ‘Committee on the Civil Dimension of Security: Enhancing the Resilience of Allied Societies Through Civil Preparedness’. Brussels, Belgium: NATO Parliamentary Assembly, 3 March 2021.
McConnell, Mike. ‘Mike McConnell on How to Win the Cyber-War We’re Losing’. *The Washington Post*. 28 February 2010.
McDermott, Rose. *Risk-Taking in International Politics: Prospect Theory in American Foreign Policy*. Ann Arbor: University of Michigan Press, 1998.
McFaul, Michael. ‘Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy’. *International Security* 45, no. 2 (1 October 2020): 95–139.
McGuinness, Damien. ‘How a Cyber Attack Transformed Estonia’. *BBC News*, 27 April 2017.
McKeon, Amanda. ‘WannaCry About NotPetya?’ *Recorded Future* (blog), 10 July 2017.
Mead, Walter Russell. ‘The Return of Geopolitics: The Revenge of the Revisionist Powers Essay’. *Foreign Affairs* 93, no. 3 (2014): [i]-79.
Mearsheimer, John. ‘Why the Ukraine Crisis Is the West’s Fault: The Liberal Delusions That Provoked Putin’. *Foreign Affairs* 93, no. 5 (2014): 77–89.
Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York ; London: Norton, 2001.
Meer, Sico van der. ‘Foreign Policy Responses to International Cyber-Attacks’. Policy Brief. Clingendael Netherlands Institute of International Relations, September 2015.
Menashri, David. ‘Iran, Israel and the Middle East Conflict’. *Israel Affairs* 12, no. 1 (1 January 2006): 107–22.
———. *Post-Revolutionary Politics in Iran: Religion, Society and Power*. London: Frank Cass, 2001.
Menn, Joseph. ‘Cyber Attacks against Banks More Severe than Most Realize’. *Reuters*, 18 May 2013.
Merom, Gil. ‘Israeli Perceptions of the Iranian Nuclear Threat’. *Political Science Quarterly* 132, no. 1 (2017): 87–118.
Meyer, Christoph O., and Eva Strickmann. ‘Solidifying Constructivism: How Material and Ideational Factors Interact in European Defence’. *JCMS: Journal of Common Market Studies* 49, no. 1 (2011): 61–81.
Miklaucic, Michael. ‘An Interview with Marina Kaljurand, Former Minister of Foreign Affairs of Estonia’. *PRISM* 7, no. 2 (2017): 116–20.
Miller, Greg, Ellen Nakashima, and Adam Entous. ‘Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault’. *The Washington Post*, 23 June 2017.
Miller, Jason. ‘Panetta Warns DoD Will Respond to Destructive Cyber Attacks’. Federal News Network, 12 October 2012.
Ministry of Defence of the Republic of Estonia. ‘National Security Concept of the Republic of Estonia (2004)’, 2004.
———. ‘National Security Concept of the Republic of Estonia (2010)’, 2010.
———. ‘National Security Concept of the Republic of Estonia (2017)’, 2017.
Ministry of Defence of the Republic of Estonia. ‘Cyber Security Strategy 2008-2013’, 2008.
Ministry of Economic Affairs of the Republic of Estonia. ‘Cybersecurity Strategy 2019-2022’. Ministry of Economic Affairs, 2018.
Ministry of Foreign Affairs of the Republic of Estonia. ‘Address by the Minister of Defence Margus Hanson As Acting Foreign Minister to the Riigikogu 15 June 2004 National Security Concept of the Republic of Estonia (2004)’. vm.ee, 15 June 2004.
———. ‘Estonia Appoints Heli Tiirmaa-Klaar as Its First Ambassador at Large for Cyber Security’. Ministry of Foreign Affairs of the Republic of Estonia, 4 September 2018.
Mirani, Leo. ‘In Case of a Russian Invasion, Estonia Is Uploading Its Government to the Cloud’. Quartz, 29 May 2014.
Mittal, Saurabh. ‘Special Issue: Cyber Complex Adaptive Systems: Methodologies, Paradigms, Tools and Technologies’. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 12, no. 2 (April 2015): 209–10.
Mitzner, Dennis. ‘Israel Prepares for #OpIsrael Cyberattack’. *TechCrunch* (blog), 4 April 2016.
Mölder, Holger. ‘Strategic Interactions of Estonia and the Implications of the Estonian Strategic Culture’. In *Strategic Decision-Making: Four Baltic Approaches*, edited by Tomas Ries, 33–76. Stockholm: Santérus Academic Press, 2014.

Mölder, Holger. ‘The Development of Military Cultures’. In *Membership: Twenty Years of Defence Development in the Baltic States*, edited by Tony Lawrence and Tomas Jermalavičius, 85–121. Tallinn, Estonia: International Centre for Defence Studies, 2013.
Mueller III, Robert S. ‘Report On The Investigation Into Russian Interference In The 2016 Presidential Election’. Washington, D.C.: U.S. Department of Justice, March 2019.
Myers, Steven Lee. ‘As NATO Finally Arrives on Its Border, Russia Grumbles’. *The New York Times*, 3 April 2004.
Myrli, Sverre. ‘Sub-Committee on Future Security and Defence Capabilities: NATO and Cyber Defence’. NATO Parliamentary Assembly, 24 November 2009.
Mythen, Gabe. ‘Reappraising the Risk Society Thesis: Telescopic Sight or Myopic Vision?’ *Current Sociology* 55, no. 6 (1 November 2007): 793–813.
Nadimi, Farzin. ‘Iran and Israel’s Undeclared War at Sea (Part 2): The Potential for Military Escalation’. The Washington Institute, 13 April 2021.
Nakashima, Ellen. ‘Biden Administration Imposes Significant Economic Sanctions on Russia over Cyberspying, Efforts to Influence Presidential Election’. *The Washington Post*, 15 April 2021.
———. ‘Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader’. *The Washington Post*. Accessed 24 February 2021.
———. ‘Cyber Command Has Sought to Disrupt the World’s Largest Botnet, Hoping to Reduce Its Potential Impact on the Election’. *Washington Post*, 10 October 2020.
———. ‘Suspected Iranian Cyberattack on American Banks Led U.S. to Rally Support of 120 International Allies’. *Washington Post*, 11 April 2014.
———. ‘U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms’. Washington Post, 27 February 2019.
———. ‘U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms’. Washington Post, 15 February 2019.
Nakasone, Paul. ‘Statement of Paul M. Nakasone Commander United States Cyber Command before the House Committee on Intelligence and Emerging Threats and Capabilities’. congress.gov, 4 March 2020.
Nakasone, Paul M. ‘A Cyber Force for Persistent Operations’. *Joint Force Quarterly*, no. 92 (January 2019): 104.
———. ‘An Interview with Paul M. Nakasone’. *Joint Force Quarterly*, no. 92 (January 2019): 104.
Nakasone, Paul M., and Michael Sulmeyer. ‘How to Compete in Cyberspace’. *Foreign Affairs*, 25 August 2020.
National Cyber Directorate. ‘Israel National Cyber Strategy In Brief’. Prime Minister’s Office, State of Israel, September 2017.
National Security Agency. ‘Iran - Current Topics, Interaction with GCHQ’, 12 April 2013.
NATO. ‘Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations’. Brussels: NATO Standardization Office, January 2020.
———. ‘Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole Militaire, Paris)’. NATO, 15 May 2018.
———. ‘Statement by the North Atlantic Council Concerning Malicious Cyber Activities’. NATO, 3 June 2020.
———. ‘Statement by the North Atlantic Council Following Meeting under Article 4 of the Washington Treaty’. NATO, 4 March 2014.
———. ‘The North Atlantic Treaty’. NATO, 4 April 1949.
———. ‘Towards the New Strategic Concept: A Selection of Background Documents’. NATO Public Diplomacy Division, April 2010.
Newman, Lily Hay. ‘The Leaked NSA Spy Tool That Hacked The World’. *Wired Magazine*, 3 July 2018.
Nichols, Thomas M. *Eve of Destruction: The Coming Age of Preventive War*. Ebook Central. Philadelphia: University of Pennsylvania Press, 2008.
Norton-Taylor, Richard. ‘Blair Sees Security Role for Russia’. The Guardian, 17 November 2001.
NTI. ‘Israel Country Page’. NTI, July 2017.

Nye, Joseph S. ‘Deterrence and Dissuasion in Cyberspace’. *International Security* 41, no. 3 (1 January 2017): 44–71.
———. ‘Neorealism and Neoliberalism’. Edited by Robert O. Keohane and Richard Rosecrance. *World Politics* 40, no. 2 (1988): 235–51.
———. *The Future of Power*. New York: PublicAffairs, 2011.
———. ‘The World Needs an Arms-Control Treaty for Cybersecurity’. Belfer Center for Science and International Affairs, 1 October 2015.
Obama, Barack. ‘Op-Ed by President Obama: Taking the Cyberattack Threat Seriously’. whitehouse.gov, 19 July 2012.
Office of Foreign Assets Control - U.S. Department of the Treasury. ‘DIRECTIVE 1 UNDER EXECUTIVE ORDER OF APRIL 15, 2021 BLOCKING PROPERTY WITH RESPECT TO SPECIFIED HARMFUL FOREIGN ACTIVITIES OF THE GOVERNMENT OF THE RUSSIAN FEDERATION’. Department of the Treasury, 15 April 2021.
Office of the Coordinator for Cyber Issues. ‘Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats’. U.S. Department of State, 31 May 2018.
Office of the Director of National Intelligence. ‘Worldwide Threat Assessment of the US Intelligence Community’, 13 February 2018.
Office of the Director of National Intelligence (ODNI). ‘Annual Threat Assessment’, 9 April 2021.
Official Website of the Department of Homeland Security. ‘About CISA’. Accessed 7 April 2020.
O’Flaherty, Kate. ‘Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First’. Forbes, 6 May 2019.
Oh, Lionel. ‘Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia’. *Cornell International Affairs Review* 12, no. 2 (2019): 121–58.
Ottis, Rain. ‘Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective’. In *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth*, 163–68. Reading: Academic Publishing Limited, 2008.
Pernik, Piret. ‘Estonian Cyber Command: What Is It For?’ ICDS, 26 November 2018.
———. ‘Responding to “the Most Destructive and Costly Cyberattack in History”’. *International Centre for Defense and Security (ICDS) Blog* (blog), 23 February 2018.
Pernik, Piret, Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, et al. ‘The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine’. HACKS, LEAKS AND DISRUPTIONS: European Union Institute for Security Studies (EUISS), 2018.
Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, Inc., Publishers, 1984.
Petersen, Karen Lund. ‘Risk Analysis – A Field within Security Studies?’ *European Journal of International Relations* 18, no. 4 (2012): 693–717.
Pew Research Center. ‘Section 2: Global Threats and Use of Military Force’. Washington, D.C.: Pew Research Center, 3 December 2009.
Phister Jr, Paul W. ‘Cyberspace: The Ultimate Complex Adaptive System’. *The International C2 Journal* 4, no. 2 (2011 2010): 32.
Piirimäe, Kaarel. ‘From an “Army of Historians” to an “Army of Professionals”: History and the Strategic Culture in Estonia’, *Scandinavian Journal of Military Studies* 3, no. 1 (2020): 100–101.
Politico. ‘Eerik-Niiles Kross: The Baltic James Bond’. Politico, 7 December 2017.
Pop, Valentina. ‘US Call for Nato Cyber-Strike Capacity Causes Division’. EU Observer, 5 October 2020.
Powell, Robert. ‘Absolute and Relative Gains in International Relations Theory’. *The American Political Science Review* 85, no. 4 (1991): 1303–20.
Prince, Conrad. ‘On the Offensive: The UK’s New Cyber Force’. RUSI, 23 November 2020.
Ralston, Patricia A.S., James H. Graham, and Jeffrey L. Hieb. ‘Cyber Security Risk Assessment for SCADA and DCS Networks’. *ISA Transactions* 46, no. 4 (1 October 2007): 583–94.
Rasmussen, Mikkel Vedby. *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press, 2006.

Raun, Toivo U. ‘Estonia after 1991: Identity and Integration’. *East European Politics and Societies* 23, no. 4 (1 November 2009): 526–34.
Record, Jeffrey. ‘Back to the Weinberger-Powell Doctrine?’ *Strategic Studies Quarterly* 1, no. 1 (2007): 79–95.
Republic of Estonia Defence Forces, ‘Military Education’, Estonian Defence Forces, 27 February 2020.
Reuters Staff. ‘Israel Says EU’s Response on Iran Recalls Nazi Appeasement’. *Reuters*, 15 July 2019.
Rhodes, Ben. *The World As It Is: Inside the Obama White House*. London: Penguin Random House, 2018.
Rice, Nikolai F. ‘Estonia’s Digital Embassies and the Concept of Sovereignty’. Georgetown Security Studies Review, 10 October 2019.
Rid, Thomas. ‘Deterrence beyond the State: The Israeli Experience’. *Contemporary Security Policy* 33, no. 1 (1 April 2012): 124–47.
Rid, Thomas, and Ben Buchanan. ‘Attributing Cyber Attacks’. *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.
Risse-Kappen, Thomas. ‘Collective Identity in a Democratic Community: The Case of NATO’. In *The Culture of National Security*, edited by Peter Katzenstein, 357–99. New York: Columbia University Press, 1996.
Roguski, Przemysław. ‘Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace’. Just Security, 6 March 2020.
Rollins, John W, Susan V Lawrence, Dianne E Rennack, and Catherine A Theohary. ‘U.S.–China Cyber Agreement’. Washington, D.C.: Congressional Research Service, 16 October 2015.
Romanosky, Sasha, and Zachary Goldman. ‘Cyber Collateral Damage’. *Procedia Computer Science* 95 (2016): 10–17.
Rosen, Stephen Peter. ‘Military Effectiveness: Why Society Matters’. *International Security* 19, no. 4 (1995): 5–31.
Ruggie, John Gerard. ‘What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge’. *International Organization* 52, no. 4 (1998): 855–85.
Ruiz, Monica M. ‘Is Estonia’s Approach to Cyber Defense Feasible in the United States?’ War on the Rocks, 9 January 2018.
Saar Poll. ‘Public Opinion and National Defence, March 2012’. Tallinn: Saar Poll, 2012.
Saddan, Nitsan. ‘Anonymous’ “Hack Israel Day” Could Impact the Entire World’. Vox, 7 April 2016.
Samani, Raj, Christiaan Beek, and Charles McFarland. ‘An Analysis of the WannaCry Ransomware Outbreak’. *McAfee Blog* (blog), 12 May 2017.
Sanger, David E. ‘Assassination in Iran Could Limit Biden’s Options. Was That the Goal?’ *The New York Times*, 28 November 2020.
———. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Scribe UK, 2018.
———. ‘U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam’. *The New York Times*, 24 March 2016.
Sanger, David E., David D. Kirkpatrick, and Nicole Perlroth. ‘The World Once Laughed at North Korean Cyberpower. No More.’ *The New York Times*, 15 October 2017.
Sanger, David E., and Andrew E. Kramer. ‘U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation’. *The New York Times*, 15 April 2021.
Sanger, David E., and Nicole Perlroth. ‘U.S. Accuses North Korea of Cyberattacks, a Sign That Deterrence Is Failing’. *The New York Times*, 26 April 2020.
Sanger, David E., Michael S. Schmidt, and Nicole Perlroth. ‘Obama Vows a Response to Cyberattack on Sony’. *The New York Times*, 19 December 2014.
Sapolsky, Harvey M., and Jeremy Shapiro. ‘Casualties, Technology, and America’s Future Wars’. *Parameters; Carlisle Barracks, Pa.* 26, no. 2 (Summer 1996): 119–27.
Schelling, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 2008.
———. *The Strategy of Conflict*. Cambridge, Massachusetts: Harvard University Press, 1960.
Schimmelfennig, Frank. ‘Arms Control Regimes and the Dissolution of the Soviet Union: Realism, Institutionalism and Regime Robustness’. *Cooperation and Conflict* 29, no. 2 (1 June 1994): 115–48.

Schmitt, Michael N., and Liis Vihul. ‘Proxy Wars in Cyberspace: The Evolving International Law of Attribution’. *Fletcher Security Review* 1, no. 2 (2014): 54–73.
Schmitt, Michael. ‘Estonia Speaks Out on Key Rules for Cyberspace’. Just Security, 10 June 2019.
Schneider, Jacquelyn G. ‘Deterrence in and through Cyberspace’. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Jon R. Lindsay and Erik Gartzke. Oxford: Oxford University Press, 2019.
Schneier, Bruce. ‘Attributing the DNC Hacks to Russia’, 9 January 2017.
Schondorf, Roy. ‘Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’. *EJIL: Talk!* (blog), 9 December 2020.
SeaNews. ‘Iran Plans to Bring Its Shahid Rajaee Port to State-of-Art Status’. SeaNews Turkey, 7 September 2019.
‘Secretary Clinton’s Meeting with Estonian Foreign Minister Urmas Paet, September 17, 2009, 2:15 P.M., Washington, D.C.’ Wikileaks Public Library of US Diplomacy. Washington, D.C: Office of the Secretary of State, 24 September 2009.
Senate Committee on Armed Services. ‘Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command’, 2014.
SentinelOne. ‘Eternalblue | How the NSA-Developed Exploit That Just Won’t Die’. *SentinelOne* (blog), 27 May 2019.
Shalal-Esa, Andrea. ‘Top General Says U.S. under Constant Cyber Attack Threat’. *Reuters*, 15 May 2013.
Shamah, David. ‘“Anonymous” a Little Less so, Thanks to Israeli Hackers’. Times of Israel, 24 May 2013.
Shapira, Itai. ‘Israeli National Intelligence Culture and the Response to COVID-19’. War on the Rocks, 12 November 2020.
Shimshoni, Jonathan. *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970*. Ithaca, NY: Cornell University Press, 1988.
Shires, James. ‘Hack-and-Leak Operations: Intrusion and Influence in the Gulf’. *Journal of Cyber Policy* 4, no. 2 (4 May 2019): 235–56.
Shushan, Inon Ben. ‘“Failed Cyber Attack on Israel Was Designed to Trigger a Humanitarian Disaster”’. JNS.org, 31 May 2020.
Siboni, Gabi. ‘Disproportionate Force: Israel’s Concept of Response in Light of the Second Lebanon War’. *INSS* (blog), 2 October 2008.
Sierzputowski, Bartłomiej. ‘The Data Embassy Under Public International Law’. *International & Comparative Law Quarterly* 68, no. 1 (January 2019): 225–42.
Siman-Tov, David, and Shmuel Even. ‘A New Level in the Cyber War between Israel and Iran’. *INSS* (blog), 3 June 2020.
Sjursen, Helene. ‘On the Identity of NATO’. *International Affairs* 80, no. 4 (2004): 687–703.
Smeets, Max. ‘NATO Allies Need to Come to Terms With Offensive Cyber Operations’. Lawfare, 14 October 2019.
Snidal, Duncan. ‘Rational Choice and International Relations’. In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse-Kappen, and Beth A. Simmons. London ; Thousand Oaks, CA: SAGE Publications, 2013.
Snyder, Jack. ‘Civil-Military Relations and the Cult of the Offensive, 1914 and 1984’. *International Security* 9, no. 1 (1984): 108–46.
Srivastava, Mehul. ‘Israel-Iran Attacks: “Cyber Winter Is Coming”’. Financial Times, 31 May 2020.
Stanley, Alessandra. ‘Russia Agrees to Full Withdrawal Of Troops in Estonia by Aug. 31’. *The New York Times*, 27 July 1994.
Stephens, Philip. ‘Cautious President Deserves Second Term’. *Financial Times*, 1 November 2012.
Stern, Jessica, and Jonathan B. Wiener. ‘Precaution Against Terrorism’. *Journal of Risk Research* 9, no. 4 (1 June 2006): 393–447.
Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge, UK: Cambridge University Press, 2016.
Stoessinger, John George. *Why Nations Go to War*. 10th ed. Belmont, CA: Thomson/Wadsworth, 2008.
Sutter, John D. ‘Anonymous Declares “cyberwar” on Israel’. CNN, 20 November 2012.

Tabansky, Lior. ‘Israel Defense Forces and National Cyber Defense’. *Connections* 19, no. 1 (2020): 45–62.
Tabansky, Lior, and Isaac Ben-Israel. *Cybersecurity in Israel*. Cham: Springer International Publishing, 2015.
Tal, David. ‘Israel’s Wars’. In *The Oxford Handbook of Israeli Politics and Society*, edited by Reuven Y. Hazan, Alan Dowty, Menachem Hofnung, and Gideon Rahat. Oxford: Oxford University Press, 2021.
Tannenwald, Nina. *The Nuclear Taboo*. Cambridge, UK: Cambridge University Press, 2007.
TBT staff and wire reports. ‘Police Conclude Probe into Alleged Riot Ringleaders’. The Baltic Times, 6 September 2007.
The Economist. ‘A Cyber-Riot’. *The Economist*, 10 May 2007.
The Hague Program for Cyber Norms. *Panel Discussion: Rethinking Cyber Espionage after the SolarWinds Hack*. YouTube, 2021.
The MITRE Corporation. ‘Matrix: Enterprise | MITRE ATT&CK™’. MITRE ATT&CK™, 2018.
———. ‘Technique: Exploitation of Remote Services - Enterprise | MITRE ATT&CK™’. MITRE ATT&CK™, 2018.
The New York Times. ‘Text: Obama’s Remarks on Cyber-Security’. *The New York Times*, 29 May 2009.
The United States Department of Justice. ‘Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System’, 16 February 2018.
———. ‘Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector’. The United States Department of Justice, 24 March 2016.
The Washington Post (courtesy of the Munich Conference on Security Policy). ‘Transcript: Putin’s Prepared Remarks at 43rd Munich Conference on Security Policy’. The Washington Post, 12 February 2007.
The White House. ‘Executive Order -- Improving Critical Infrastructure Cybersecurity’. whitehouse.gov, 12 February 2013.
———. ‘FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government’. The White House, 15 April 2021.
———. ‘International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World’, May 2011.
———. ‘National Cyber Strategy of the United States of America’. Washington, D.C.: The White House, September 2018.
———. ‘Statement from the Press Secretary’, 15 February 2018.
———. ‘National Security Strategy’, May 2010.
———. ‘National Security Strategy’, February 2015.
———. ‘National Security Strategy of the United States of America’. The White House, December 2017.
———. ‘Press Conference by the President’. whitehouse.gov, 16 December 2016.
———. ‘Report on Cyber Deterrence Policy’. federalnewsnetwork.com, 2015.
———. ‘Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment’. whitehouse.gov, 29 December 2016.
———. ‘Report on Cyber Deterrence Policy’, 2015.
———. ‘The National Security Strategy of the United States of America’. Washington, D.C: The White House, September 2002.
———. ‘U.S. National Security Strategy’. fas.org, 20 May 1982.
Tierney, Dominic. ‘The Obama Doctrine and the Lessons of Iraq’. Foreign Policy Research Institute (FPRI), May 2012.
Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.
Tisdall, Simon ‘Mogadishu Outrage Puts Clinton in Firing Line’, The Guardian, 5 October 1993,
TOI staff. ‘Israeli Sites Hacked to Display: “Jerusalem Is the Capital of Palestine”’, 4 April 2018.

Tooze, Adam. ‘The Sociologist Who Could Save Us From Coronavirus’. Foreign Policy, 1 August 2020.
Tor, Uri. ‘“Cumulative Deterrence” as a New Paradigm for Cyber Deterrence’. *Journal of Strategic Studies* 40, no. 1–2 (2017): 92–117.
Traynor, Ian. ‘Russia Accused of Unleashing Cyberwar to Disable Estonia’. The Guardian, 17 May 2007.
———. ‘Russia and Nato Reach Historic Deal’. The Guardian, 15 May 2002.
Tucker, Eric. ‘US, Estonia Partnered to Search out Cyber Threat from Russia’. AP NEWS, 3 December 2020.
Tulloch, John, and Deborah Lupton. *Risk and Everyday Life*. London: Sage, 2003.
Tversky, Amos, and Daniel Kahneman. ‘Judgment under Uncertainty: Heuristics and Biases’. *Science* 185, no. 4157 (27 September 1974): 1124–31.
United States Army. ‘Cyberspace Operations Concept Capability Plan 2016-2028’. Department of the Army, United States of America, 22 February 2010.
United States Holocaust Memorial Museum. ‘Press Guide to Holocaust Denial in Iran’. Accessed 28 January 2021.
U.S. Cyber Command. ‘Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command’. United States Cyber Command, 2018.
———. ‘Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation’. U.S. Cyber Command, 3 December 2020.
U.S. Department of Defense. ‘Department of Defense Strategy for Operating in Cyberspace’, July 2011.
———. ‘Secretary of Defense Speech: Retirement Ceremony for General Keith Alexander’. Defense.gov, 28 March 2014.
———. ‘The Department of Defense Cyber Strategy’. Department of Defense, April 2015.
———. ‘Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City’. U.S. Department of Defense, 11 October 2012.
U.S. Department of Homeland Security. ‘Written Testimony of NPPD for a Senate Committee on Armed Services Hearing Titled “Roles and Responsibilities for Defending the Nation from Cyber Attack”’. Department of Homeland Security, 19 October 2017.
U.S. Department of State. ‘Responding to Modern Cyber Threats with Diplomacy and Deterrence: Remarks Dr Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Center for Strategic and International Studies, Washington DC’. United States Department of State, 19 October 2020.
U.S. Department of the Treasury. ‘Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups’. U.S. Department of the Treasury, 13 September 2019.
———. ‘Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks’. U.S. Department of the Treasury, 15 March 2018.
———. ‘Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury’, 15 March 2018.
U.S. Embassy in Estonia. ‘Estonia: Das Quanrud Discusses Afghanistan, Russia, the Economy’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 16 December 2009.
———. ‘Estonia: GOE Officials on the Bronze Soldier, Russia and Integration’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 11 May 2007.
———. ‘Estonia: Scenesetter for Visit of DHS Secretary Chertoff’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 23 October 2008.
———. ‘Russian Bear Hug Squeezes Estonian Economy’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 29 May 2007.
———. ‘Scenesetter for A/S Fried’s Visit to Estonia’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 25 September 2008.
———. ‘USG Support for Estonian Cyber Center (Corrected Copy - Added Addressee)’. Wikileaks Public Library of US Diplomacy. Tallinn, Estonia: U.S. Embassy in Estonia, 7 February 2008.

US Naval War College. *2019 Future Warfighting Symposium: Emily Goldman, Cyber Strategy and Policy*. Newport, RI, 2019.
USCYBERCOM Malware Alert. 'Malware Attributed to #NorthKorea by @FBI_NCIJTF Just Released Here: Https://T.Co/CBqSL7DJzI. This Malware Is Currently Used for Phishing & Remote Access by #DPRK Cyber Actors to Conduct Illegal Activity, Steal Funds & Evade Sanctions. #HappyValentines @CISAgov @DHS @US_CYBERCOM'. *Twitter* (blog), 14 February 2020.
Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.
Van Evera, Stephen. 'The Cult of the Offensive and the Origins of the First World War'. *International Security* 9, no. 1 (1984): 58–107.
Vass, Lisa. 'North Korean Programmer Charged for Sony, WannaCry Attacks and More'. *Naked Security by Sophos* (blog), 10 September 2018.
Vavra, Shannon. 'Cyber Command Deployed Personnel to Estonia to Protect Elections against Russian Threat'. CyberScoop, 3 December 2020.
———. 'Pentagon, FBI, DHS to Jointly Expose a North Korean Hacking Effort'. CyberScoop, 14 February 2020.
Verdaasdonk, Willem. 'Data Embassies: How Estonia Might Pave The Way For Reducing Uncertainty In Cyberspace'. *Leiden Security and Global Affairs Blog* (blog), 25 November 2019.
Vital, David. *The Survival of Small States: Studies in Small Power/Great Power Conflict*. London: Oxford University Press, 1971.
Volz, Dustin. 'Trump Administration Says Russia Likely Behind Massive SolarWinds Hack'. *Wall Street Journal*, 6 January 2021.
———. 'Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive'. *Wall Street Journal*, 16 August 2018.
Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. 'National Cyber Power Index 2020'. China Cyber Policy Initiative. Boston, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, September 2020.
Wæver, Ole. 'Securitization and Desecuritization'. In *On Security*, edited by Ronnie Lipschutz, 46–86. New York: Columbia University Press, 1995.
Wallander, Celeste, and Robert Keohane. 'Risk, Threat, and Security Institutions'. In *Imperfect Unions: Security Institutions over Time and Space*, edited by Helga Haftendorn, Robert Keohane, and Celeste Wallander, 21–47. Oxford: Oxford University Press, 1999.
Walt, Stephen M. 'Alliance Formation and the Balance of World Power'. *International Security* 9, no. 4 (1985): 3–43.
———. 'Rigor or Rigor Mortis?: Rational Choice and Security Studies'. *International Security* 23, no. 4 (1999): 5–48.
Waltz, Kenneth N. 'Realist Thought and Neorealist Theory'. *Journal of International Affairs* 44, no. 1 (1990): 21–37.
———. *Theory of International Politics*. New York ; London: McGraw-Hill, 1979.
———. 'Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability'. *Foreign Affairs* 91, no. 4 (2012): 2–5.
Warrick, Joby, and Ellen Nakashima. 'Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran'. *Washington Post*, 8 May 2020.
———. 'Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility'. *Washington Post*, 18 May 2020.
Waterman, Shaun. 'Clapper: U.S. Shelved "hack Backs" Due to Counterattack Fears'. CyberScoop, 2 October 2017.
Weber, Max. *On the Methodology of the Social Sciences*. Philadelphia, Pennsylvania: The Great Library Collection by R.P. Pryne, 1949.
Weiss, Michael. 'The Hero Who Betrayed His Country'. *The Atlantic*, 26 June 2019.
Wendt, Alexander. 'Anarchy Is What States Make of It: The Social Construction of Power Politics'. *International Organization* 46, no. 2 (1992): 391–425.

———. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
Whitelaw, Kevin. ‘Ahmadinejad: Holocaust “Opinion Of Just A Few”’. NPR.org, 25 September 2009.
Whyte, Christopher. ‘Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online’. *European Journal of International Security* 5, no. 2 (June 2020): 195–214.
Wilkinson, Iain. *Anxiety in a Risk Society*. London: Routledge, 2001.
Williams, Michael C., and Iver B. Neumann. ‘From Alliance to Security Community: NATO, Russia, and the Power of Identity’. *Millennium* 29, no. 2 (1 June 2000): 357–87.
Williams, Michael J. ‘(In)Security Studies, Reflexive Modernization and the Risk Society’. *Cooperation and Conflict* 43, no. 1 (2008): 57–79.
———. *NATO, Security and Risk Management: From Kosovo to Kandahar*. Contemporary Security Studies. London ; New York: Routledge, 2010.
———. *NATO, Security and Risk Management: From Kosovo to Kandahar*. Contemporary Security Studies. London ; New York: Routledge, 2010.
Wimmer, Jeffrey, and Thorsten Quandt. ‘Living in the Risk Society: An Interview with Ulrich Beck’. *Journalism Studies* 7, no. 2 (1 April 2006): 336–47.
Wirtz, James J. ‘How Does Nuclear Deterrence Differ from Conventional Deterrence?’ *Strategic Studies Quarterly* 12, no. 4 (2018): 58–75.
Witko, Christopher. ‘How Wall Street Became a Big Chunk of the U.S. Economy — and When the Democrats Signed On’. *Washington Post*, 29 March 2016.
Wolf, Alexander. ‘US Interventions Abroad: A Renaissance of the Powell Doctrine?’ *Strategic Studies Quarterly* 3, no. 4 (2009): 125–39.
Work, JD, and Richard Harknett. ‘Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges’. Issue Brief. Washington, D.C.: Atlantic Council Scowcroft Center for Strategy and Security, July 2020.
Wright, Jeremy. ‘Speech: Cyber and International Law in the 21st Century’. GOV.UK, 23 May 2018.
Wulf, Meike. *Shadowlands: Memory and History in Post-Soviet Estonia*. New York: Berghahn Books, 2016.
Yin, Robert K. *Case Study Research and Applications: Design and Methods*. Sixth edition. Thousand Oaks, California: SAGE Publications, Inc, 2018.
Zegart, Amy. ‘Everybody Spies in Cyberspace. The U.S. Must Plan Accordingly.’ The Atlantic, 30 December 2020.
Zetter, Kim. ‘Hacker Lexicon: What Are CNE and CNA?’ *Wired*, 7 June 2016.
———. ‘The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks’. *Wired*, 2 October 2015.