JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–15
https://doi.org/10.1093/cybsec/tyab014
Research paper

Research paper

Cyber legalism: why it fails and what to do about it

Lucas Kello*

Department of Politics and International Relations, University of Oxford, Manor Road Building, Manor Road, Oxford OX1 3UQ, UK

*Correspondence address: Department of Politics and International Relations, University of Oxford, Manor Road Building, Manor Road, Oxford OX1 3UQ, UK. Tel: +44-1865-278700; E-mail: lucas.kello@politics.ox.ac.uk

Received 12 September 2021; revised 17 January 2021; accepted 22 April 2021

Abstract

Western nations face a glaring punishment problem in the cyber domain. Repeatedly, other nations assail their political and economic interests. Repeatedly, Western leaders warn about the gravity of such actions. And yet repeatedly, the victims failed to punish to deter the offenders. This article examines why and how this situation arose and what to do about it. The Western approach to cyber conflict prevention emphasizes the centrality of existing international law and norms. The legal and normative framework is not adequate for this purpose, however, because it does not provide sufficient grounds to credibly respond to actions falling short of war. Consequently, the Western approach has failed spectacularly. It fails to grasp a central truth about contemporary security affairs: much of modern interstate rivalry fits neither the destructive criteria of war nor the acceptable boundaries of peaceful rivalry. Rather, it is *unpeace*, or mid-spectrum rivalry that is more damaging than traditional peacetime activity, but not physically violent like war. Nations use cyberspace to achieve some of the political and strategic objectives of war without firing a single gun. The lack of an effective Western response betrays not tolerance of aggression but a failure to devise a response strategy commensurate with the legal and doctrinal ambiguities of unpeace. Existing law and norms are a source of the problem, not its solution. An interim solution must be found instead in the development of new doctrine—in a consequentialist strategy that affects adversaries' material interests to deter actions which international law and security strategy do not ordinarily recognize as deserving a strong response.

Key words: strategy, policy, international relations, deterrence, norms

The Punishment Problem

Western nations face a glaring punishment problem in the cyber domain. Repeatedly, other nations assail their political and economic interests. Repeatedly, Western leaders warn about the gravity of such actions. The White House depicted the Sony Pictures hack in 2014 as a "serious national security matter" [1]. National Security Advisor John Bolton described Russia's public release of hacked email records of the Democratic Party during the 2016 US presidential election as "an act of war against our constitutional structures" [2, page 174]. The head of Britain's MI6 spy agency warned that the manipulation of social media by foreign powers during the "Brexit" referendum presented "a fundamental threat to our [nation's] sovereignty," adding: "They should be a concern to all those who share democratic values" [3]. French President Emmanuel Macron decried Russian state hackers' release of private emails belonging to his campaign staffers in 2017 as an attempt at "democratic destabilization" during a presidential election [4]. Amid the Covid-19 pandemic, European Commission President Ursula von der Leyen chastised China for intruding upon European public health infrastructures, warning that such behavior "cannot be tolerated" [5].[1]

1 The term "Western" in this article refers to the liberal democratic states of Europe and North America as well as politically and culturally related countries such as Australia. Although cyber threats affect many other nations (including democratic ones), the article focuses on Western states because of their shared political values, common strategic traditions, and a history of close cooperation in political, economic, and security affairs

And yet repeatedly, Western nations failed to punish to deter the offenders. President Barack Obama promised firm penalties against North Korea; only weak economic sanctions ensued. In 2016, he publicly rebuked Russia for the DNC hack, but merely expelled some of its diplomats and issued narrowly targeted financial sanctions. "The punishment did not fit the crime," lamented former US ambassador to Russia Michael McFaul. "Russia violated our sovereignty, meddling in one of our most sacred acts as a democracy—electing our president. The Kremlin should have paid a much higher price for that attack. And US policymakers now—both in the White House and Congress—should consider new actions to deter future Russian interventions" [7]. Another Obama Administration official similarly criticized his government's response: "[It] is the hardest thing about my entire time in government to defend. I feel like we sort of choked" [8]. Macron's foreign policy advisor warned that France had "a doctrine of retaliation when it comes to Russian cyber attacks," adding ominously: "We are ready to retaliate to cyberattacks not just in kind but with any other conventional measure…." [9]. Yet no punishment ensued for the intervention in the election; authorities did not even attempt to intimidate the hackers' by revealing their identities, which over time could help to build stable reputations of behavior [10]. So far, the European Union (EU) has not levied any penalties for the health system intrusions. Riven by internal division, the EU remains largely quiescent against Chinese and other foreign threats, sanctioning for example just a small number of individuals and organizations for incidents as significant as "Operation Cloud Hopper," a multiyear Chinese espionage campaign targeting private corporations on six continents [11,12]. Meanwhile, some EU member states continue to source vital communications infrastructure components from Huawei and other Chinese companies despite warnings of compromise [13].

In the highly classified cyber domain where states often operate covertly, whether because divulging an operation's existence can reveal the vulnerabilities it exploits in the adversary's systems, or because the attacking nation does not want to attract political and diplomatic attention, it is possible that some punishments are publicly unobservable. But researchers must formulate their analysis on the basis of available evidence; or if they will entertain a conjecture, they must extrapolate from evidence in relevant incidents. Fourteen years have transpired since Western nations began to experience strategic level cyberattacks by other states or their sympathizers.[2] Has new evidence emerged showing sterner responses than previously known? So far, no. No new information has revealed major punishments for the actions against Sony Pictures or against US and French democratic institutions or for other notable incidents. Until such evidence emerges, analysts must assume that governments have not secretly punished cyber activity more firmly than has been observed. At any rate, secret punishment would complicate third-party deterrence: it weakens the message to other aspiring attackers (on which more below). A former senior British government official questioned the thesis of covert punishment in cyberspace: "Very often, nothing is said about a response—not because it was classified, but because nothing actually happened."[3]

The West in short suffers a problem of *under-proportionate response*: it fails to punish cyber actions sufficiently hard to convince adversaries that the retaliatory costs outweigh the gains. Officials are aware of the problem. A clear recognition was articulated in 2017 by US Senator John McCain: "[W]e don't have a policy and we don't have a strategy," he said in relation to Russia's politically disruptive cyber activity. "[I]t is the one aspect of our confrontation where I believe our adversaries are ahead of us" [15]. About the threat posed by Russia and China, US Director of National Intelligence Daniel Coats stated in 2018: "These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations" [16]. Governments have not sat idly by. Foreign culprits have been indicted, sanctions have flowed, disabling preemptive measures have struck—for example, during the US mid-term elections in 2018, Cyber Command disrupted the Russian Internet Research Agency's network connection [17]. Yet the responses have not significantly diminished the intensity of offensive action. Aggressors are often named but rarely shamed, sternly rebuked but only meekly punished, harassed but largely undeterred.

The apparent success of deterrence against true acts of cyberwar is a notable achievement, especially in light of naïve warnings of a "Cyber 911" or a "Cyber Pearl Harbor" [18]. But below the threshold of war, adversaries have not been rebuffed forcefully enough to prevent further ordeals. In July 2019, Microsoft reported that Russian and North Korean actors conducted political hacking activities against presidential campaign targets in the United States. Three months later, the company warned that state-backed Iranian hackers targeted the email accounts of almost 3000 US government officials, presidential campaign officers, and journalists. US officials considered striking Iran's computer infrastructure in retaliation; evidence for such action actually having taken place does not exist [19]. Even after suffering a slew of financial sanctions and criminal indictments between 2016 and 2020, Russian state hackers continued to penetrate the United States' most prized governmental systems. In one major incident, the "SolarWinds" intrusion, authorities suspected the presence of Russian hackers in thousands of computers in more than a dozen federal departments and agencies. Joe Biden used the opportunity of his first phone call as president with Vladimir Putin to protest against the intrusions; even so, prominent former officials and analysts warned about hitting back too hard or at all [20]. The failure to carry out dissuasive repercussions in the cyber domain endures as a sore point of Western security policy.

Why and how this situation arose, and what to do about it, is the subject of this article. To anticipate the central diagnosis, Western responses have emphasized the centrality of existing international law and norms in regulating cyber conduct. They perceive the legal framework as a tool to introduce predictability and reduce risk in an unruly domain of conflict [21]. Let us call this approach *cyber legalism* for its attachment to the appurtenances of the legal system. It has failed spectacularly. The current legal and normative framework is not adequate for the purpose that Western policymakers ascribe to it, because it does not provide sufficient grounds to credibly respond to offensive actions falling short of war. Legal scholars have made much progress in evaluating how legal and ethical standards of proportionality and discrimination apply in cyber conflict [22–26]. But there are glaring gaps in thinking and practice, especially on the question of the relationship between legal doctrine and security doctrine—how a particular interpretation of the former constrains the latter's development. What is required is a pragmatic benchmark of cyber response that focuses not an building an ideal world but on achieving results: the successful prevention of future hostile actions,

within institutions such as NATO, the European Union, and the Five Eyes community, which together envelop the family of Western nations. On the commonalities of Western strategic thinking and practice, see [6].

2 The unsophisticated but disruptive attacks against Estonia's financial and governmental computer systems in 2007 were "a virtual demonstration shot" that elevated cyber threats to the top of many countries' national security agenda. See [14, page 212].

3 Author interview, November 27, 2019.

not merely above the war threshold, where deterrence is working, but also below it, where current policy fails routinely to prevent damage against economic infrastructures and democratic institutions. The existing legal order does not supply a framework on which to build policy that satisfies such a benchmark.

The solution to contemporary security problems, therefore, must be found not in law and norms primarily but in the refinement of *doctrine*: figuring out how to respond to activity—in order to deter its recurrence—that international legal traditions and security strategy do not ordinarily recognize as punishable. Doctrine comprises a synthesis of understandings about the strategic environment: how to relate technological possibility, adversarial intentions, and one's own resources to the pursuit of valid goals without committing or risking too much. This collection of understandings is organized—sometimes formally, other times only implicitly, but always influentially—into a rulebook of assumptions, principles, and goals that guides policymakers' pursuit of interests amid the uncertainties of an anarchic international environment.[4] Enduring flaws in doctrine, however, have impeded the adaptation of security strategy to cyber threats.

The remainder of the article proceeds in five steps. First, it reviews the effect of new technology on the nature and methods of modern conflict, which increasingly occurs below the war threshold. Second, it discusses the limitations of the existing legal and normative framework—from which much of Western security strategy draws—in addressing the challenge of cyber conflict prevention. Third, it asks whether legal talk is just cheap talk to serve national interests. Fourth, it exposes the flaws in the universalistic assumptions of cyber legalism. Fifth, it briefly examines how a consequentialist punishment strategy grounded in calculations of material interests could overcome existing policy shortcomings and proposes principles to guide its development. The scope of the article's analysis does not cover scenarios in which cyber actions support or satfisfy the criteria of conventional war or a use of force.[5] Such scenarios would implicate traditional laws governing armed conflict and territorial violations of sovereignty; they would not invoke the legal and strategic conundrums that this article addresses.

Modern Conflict: War, Peace, and Unpeace

The main source of Western policy paralysis is a failure to grasp the changing tides of modern conflict. Traditionally, war has been the principal force of change in international affairs. The First World War consumed three historical empires—Tsarist Russia, Imperial Germany, and Austria-Hungary—out of whose remains emerged the twentieth century's two transforming ideologies, communism and fascism. The Second World War crushed the European great powers that had dominated world politics for centuries, enabling the appearance of two non-European superpowers in the twentieth century, the United States and the Soviet Union.

The current era is different. The relevance of war to historical transformation has diminished. War no longer alters history as it did in the past. War today plays an essentially conservative function: it preserves the existing international order more than undermining it. True, some world leaders (think of the dictator in Pyongyang) behave as if the choice of arms still existed. And in some regions such as the Middle East (consider Syria or Yemen), civil war and armed intervention endure as a blight of diplomacy [29–33]. But when war occurs, it mainly seeks to uphold the international order, as in the First Iraq War (to correct the transgression of Saddam Hussain's invasion of Kuwait) or NATO's air campaign against Libya (to stop Muammar Gaddafi's violent suppression of civilian protestors). Relative to the rich history of warfighting, the most distinctive feature of conflict in the current century is the silencing of guns among large nations. Their leaders grasp that even a minor armed confrontation among them is almost inconceivable because its consequences would be economically and politically ruinous. In the present era, large powers threaten war primarily to avoid it.

Less war does not mean more peaceful means of rivalry, however. These too have waned in relevance. All of the cyber incidents described earlier share a defining characteristic: their cumulative effects inflicted greater political or economic damage than even some isolated acts of conventional war, yet their nonviolent nature placed them below war's legal and institutional criteria. The incidents, it is harder but equally—perhaps more—important to realize, also violated the definition of peace: the state of restrained rivalry (if not comity) that statesmen normally aspire to achieve in the midst of international anarchy. Not long ago, some analysts optimistically celebrated the emergence of an era of "cyber peace" marked by tolerable acts of minor aggression [34] (more on peace later). True, nonviolent cyber actions may present states with viable alternatives to real war, such as the use of weaponized code instead of conventional airstrikes to destroy nuclear enrichment centrifuges in Iran.[6] Others, however, enable more damaging forms of conflict below that threshold: for example, the disruption of a small country's financial infrastructure or a large nation's democratic election remotely and surreptitiously, which would be difficult to achieve with arms of war. The statements of leaders cited earlier reveal that they do not tolerate such aggression, which they nevertheless struggle to punish. The absence of major war among geopolitical opponents cannot obscure the fact that we live in a period of intense technological rivalry—one that Western nations are losing.

Western policymakers fail to grasp a central truth: much of modern interstate rivalry fits neither the destructive criteria of war nor the acceptable boundaries of peace. Rather, it is *unpeace*, or mid-spectrum rivalry that is more damaging than traditional peacetime activity (such as economic sanctions), but not physically violent like war [14]. Although states have conducted sabotage, assassinations, special operations, and covert action throughout history, unpeace is different because direct forms of violence do not occur nor are threatened—and yet significant harm to interests occurs.

Because cyberspace is an intelligence-rich domain, some thinkers have fallen into the temptation of analogizing cyber unpeace with the logic of state espionage [36]. Important differences exist in the activity's scale (think of NotPetya's disruption of global shipping), remoteness (imagine foreign agents infiltrating vital infrastructure on the national soil without actually being there), and variety of threat actors (consider the vast universe of state and non-state players with possibly unknown motives and aims who participate in some large cyber operations). But there is more. Cyberspace is altering the aims and methods of espionage. In the traditional logic of espionage, stolen information generally loses its value the more it is shared or publicly disclosed. Although much espionage in cyberspace seeks to remain in

4 Doctrine has more than one form. It can be declaratory, or what policymakers want their actions to look like, and operational, or how actors actually behave. See [27]. Or as J. David Singer put it, a state's "official or articulated ideology" can differ from its "operative ideology" [28].

5 An example of such a scenario is the distributed denial-of-service attacks that interrupted Georgia's central bank operations during the country's military invasion by Russia in August 2008.

6 For this reason, Duncan Hollis believes that in some instances there is a "duty to hack" in international politics [35].

the shadows (as in the SolarWinds and Microsoft Exchange hacks), increasingly it willingly comes to light. Not content with merely using stolen secrets quietly, adversaries increasingly seize information to reveal it publicly, such as in so-called kompromat or hack-and-leak operations [37]. And that is the point: to release stolen information publicly in order to cause political or social harm. In relation to conventional intelligence gathering, then, some forms of cyber espionage represent a difference in kind and not in degree. Rather than being shaped and constrained by the traditional logic of intelligence gathering, developments in cyberspace alter it.

In these circumstances, the absence of war no longer means the prevalence of peace. The technological methods of unpeace have become more relevant forces of change in international politics than war itself. Nations can use cyberspace to achieve some of the main political and strategic objectives of war without firing a single gun [14, 38]. The lack of deterring penalties betrays not tolerance of aggression but a failure to devise a response strategy commensurate with the legal and doctrinal peculiarities of unpeace.

Yet the rigid thinking about war and peace prevails in Western capitals. To be sure, the reality of unpeace is increasingly recognized. As US Cyber Command noted: "Adversaries continuously operate against us below the threshold of armed conflict. In this 'new normal,' our adversaries are extending their influence without resorting to physical aggression. They provoke and intimidate our citizens and enterprises without fear of legal or military consequences [39, page 3]." But the development of new doctrine to guide behavior in the new genus of conflict remains primitive, even if its legal and normative enterprise is robust—precisely because the West is so behind in doctrinal ingenuity. Because security policy still operates mainly within the bounds of the peace-war binary, yet much of security competition is neither one nor the other, these policies produce seriously flawed results. Western understandings of modern conflict either prioritize the language of war or fuse war and peace into a single, convoluted phenomenon. The vague term "hybrid war" that mars much doctrinal writings illustrates this flawed conception. The term ordinarily denotes the combination of war and nonviolent means of conflict, often by a mix of state actors and private citizens acting with or without their government's direction, such as in the cyberattacks against the central bank of Georgia in August 2008 during the country's military invasion by Russia [40–42]. It offers little analytical value; the existence of conventional acts of war situates the scenario, legally and politically, within the framework of war. If, however, the term denotes actions that are not traditionally warlike, then it merely emphasizes what we already knew: that the activity is not violent, in which case the term hybrid "war" itself is misleading.

Slogans of "warfare during peacetime" that are popular among Western politicians are similarly flawed. The 2016 Republican Party Platform declared: "Russia and China see cyber operations as a part of a warfare strategy during peacetime" [43]—a splendid fallacy, for war and peace are definitionally exclusive. Such utterances hold intuitive appeal because the activity in question is neither warlike nor peaceful—but nor, logically, can it be both at once. Other examples of conceptual acrobatics are "next-generation warfare" and "nonlinear warfare," terms for information operations that are popular among Russian military thinkers. They, too, are misleading—perhaps purposefully so. The activity appeals to Russian strategists precisely because its nonviolent methods fall short of war, even as they often surpass the tolerable limits of peacetime competition. Analytically, the blurring of the concepts of war and peace is sloppy; policy-wise, it is a formula for disaster.

Against the backdrop of policy failures, another argument of this article may rattle Western officials: Russia and China are the masters of the modern methods of technological conflict. Russia's intrepid actions in particular reveal the superiority of its security doctrine in an era of unpeace. Strategists in Moscow grasp two essential truths better than their Western counterparts: in the twenty-first century, disruptive cyber methods can achieve greater strategic effect than the destruction of war; and so long as their physical effects do not rise to the level of war, the actions will largely go unpunished [14].

Law and Norms: Sources of the Problem, Not the Solution

Western attempts to curtail cyber conflict have focused on the preferred methods of Western diplomacy: the fostering of laws and norms of responsible state conduct. Officials wedded to the doctrine of cyber legalism stress the importance of existing international law and institutions to prevent hostile actions. They emphasize the value of forums such as the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), which explore how legal conventions such as the UN Charter principles apply to the regulation of cyber conduct (a central point of contention among participating nations). They stress the reasonableness of prevailing norms, as if the transgressors in Moscow or Pyongyang had failed for all these years to grasp their self-evident validity.[7]

The existing legal framework reinforces the traditional peace–war binary that underpins Western security doctrine. As former general counsel to US Cyber Command Gary Corn observed: "International law comes down on the side of Clausewitz. It draws some fairly bright lines. The distinction between armed conflict and non-armed conflict is stark, because once you cross that Rubicon, you are able to kill based solely on a person's status, not his or her immediate conduct."[8] But cyber conflict often occurs along a spectrum *between* the poles of war and peace [49]. Thus, the legal order in which Western officials search for solutions to the challenge of cyber conflict prevention in fact impedes them. The binary thinking that underpins the legal framework (Give us war or give us peace for anything in between we struggle to interpret!) hinders the refinement of doctrine for a new era of conflict. It offers no or few clear benchmarks to guide the response to technological acts of unpeace.

Western policy in brief demands of the existing legal order more than it can presently give. From the clash of legal interpretation and doctrine on the one side and the new realities of conflict on the other emerges a posture of inaction or weak action that is characteristic of policymaking in times of technological revolution. As Corn aptly put it: "What the ambiguities of the grey zone do is create decision delay and often paralysis because of uncertainty in the legal interpretation of actions."[9]

This argument does not deny the important advances in global cooperation over technical aspects of the Internet—even on the backdrop of a contest among governance models. The open model championed by Western nations and early Internet pioneers seeks to preserve nearly unfettered information exchange, that is, away from the prying eyes and censoring arm of the government. A competing

7 The topic of law and norms of interstate cyber conduct has received growing attention within political science and international relations. See, for example, [44–48].

8 Author interview with Gary Corn, March 3, 2021.

9 Interview with Corn. It is important to realize that unpeace and the "grey zone," as analysts commonly use the term, are not the same. Although both notions denote offensive action that falls between the extremes of war and peace, unpeace is narrower because its consequences are not directly violent or fatal (while not all forms of violence are necessarily acts of war).

closed model (or models, if one considers differences among Russian, Chinese, and other authoritarian "intranets" [50]) implements stringent information controls and surveillance. Yet despite the clash of models, which increasingly plays out in nations and regions (think of Africa) not yet wedded to one or the other approach, cooperation at the technical level (for example, over IPv6 deployment) has been successful. Functionally speaking, the Internet remains a largely interoperable realm. Indeed, possibly it is too interoperable: the ease of information exchange between machines (especially in the open Internet) facilitates the acts of unpeace that mar cyberspace. In sum, although interstate cooperation over cyber conflict remains poor, cooperation over technical Internet matters has seen relative success [51–53].

The United States is among the chief proponents of cyber legalism. In 2010, not one year after the establishment of US Cyber Command, its first commander General Keith Alexander affirmed before the Senate during his confirmation hearing: "[Department of Defense] operations are conducted consistent with international law principles in regard to what is a threat or use of force in terms of hostile intent and hostile act" [54–56]. As if a vow of obedience to international law was a prerequisite of the job, Alexander invoked UN Charter principles—especially the principle of self-defense—as guiding lights of policy. Similarly, Defense Secretary Chuck Hagel stated in 2014 that his country "will maintain an approach of restraint to any cyber operations outside of U.S. government networks" [57]. General Paul Nakasone, Alexander's current successor, and senior advisor Michael Sulmeyer reaffirmed: "[U.S.] cyber forces abide by widely accepted principles of international law, and when they take direct action, they narrowly tailor the effect," emphasizing the laws of war: "[O]ur actions must also remain consistent with the law of armed conflict and other important international norms" [58]. This policy course follows the direction set by the first US International Strategy for Cyberspace, which expressed a commitment to build a "global consensus" around norms of conduct drawing from existing international law [59]. Constructing the consensus was a chief task of Christopher Painter, the first US Coordinator for Cyber Issues who assiduously pursued his remit in "a new area of foreign policy" within multilateral forums.[10] Diplomats have pursued consensus particularly within the UNGGE, a vehicle of norm construction (or more often norm contestation) drawing from existing international law whose efforts the United States initially underplayed but today champions [61–63].

Recent US policy changes that adopt a more assertive posture nevertheless seek to respect (or be seen to respect) the rigid adherence to law. The new policy of "persistent engagement" paves the way for more intrusions in adversaries' home networks—for example, searching through or disabling foreign computers to impede offensive moves. Persistent engagement is a refinement of the older notion of "active defense," whose defining characteristic was out-of-perimeter activity [64]. But as a manifestation of the doctrine of "defending forward," the policy operates within the broad realm of self-defense. It manifestly does not prescribe offensive action for deterrence purposes. Rather, it seeks "to disrupt and degrade the capabilities our adversaries use to conduct attacks" [58]—that is, to undermine the attack by imposing costs on attackers but not to penalize them [65, 66].

Allies and close partners of the United States also espouse the mantra of cyber legalism. In 2019, Britain endorsed a commitment to "law, norms, and confidence building in cyberspace" [67]. Echoing Painter's mission, the British national cyber strategy emphasized the aim of building a "global alliance" promoting the respect of international law in cyberspace [68]. EU officials have toed a similar line. Drawing from their union's record of pacifying a continent where for centuries the resort to war was an accepted device of statecraft and the quest for domination its occasional aim, EU officials pride themselves on Europe's status as a "normative power" that can uphold the international (or at least regional) order and resolve interstate quarrels peacefully [69]. In 2019, EU foreign policy chief Federica Mogherini expressed the union's aspiration of becoming "a forward-looking cyber player," for which policymakers devised a "toolbox" of measures, including punitive economic sanctions, to strengthen "the rules-based order in cyberspace, including the application of international law and the adherence of norms of responsible state behaviour" [70]. NATO too has chimed in. Responding to malicious intrusions targeting public health infrastructure during the Covid-19 pandemic, for example, the alliance's governing council declared: "We all stand to benefit from a rules-based, predictable, open, free, and secure cyberspace" [71].

Cyber legalism, in sum, is not an emerging or debated approach within Western policy circles; it is the central thrust of the approach to conflict reduction. It represents an expansive normative program, one in which, at least implicitly, the familiar corpus of principles, rules, and norms that were developed to constrain war in other domains of conflict should also apply, in some as yet undefined and contested but sorely needed way, to constrain damaging actions below its threshold.

Is Legal Talk Just Cheap Talk?

Cynics may see in these pronouncements a subterfuge of large nations and the organizations they control to cloak power politics in the legitimacy of international law.[11] After all, soon after affirming in the Senate a commitment to legal constraints, Alexander presided over the most destructive cyberattack on the record, the so-called Olympic Games operation that destroyed almost 1000 uranium enrichment centrifuges in Iran, an act that some observers have regarded as an illegal use of force [74]. Or else, large adversaries may perceive cyber legalism as a tool of Western "normative imperialism," an attempt to impose a liberal vision of international affairs in a poorly defined realm of action that offers dominant players many imperialistic spoils [75].

These cynical views resonate with the "cheap talk" theory of international rhetoric in which leaders use moral language as a ruse to

10 Painter's biography at Stanford University states: "His efforts helped create a new area of foreign policy focus that included promoting norms of responsible state behavior and cyber stability…. He and his team also spearheaded the promotion of an international framework of cyber stability that includes building a consensus around norms of acceptable behavior…." [60].

11 The question of the relationship between national power and international law is the subject of much debate. Jack Goldsmith and Eric Posner argued that states comply with international law for instrumental reasons. As they put it: "the possibilities for what international law can achieve are limited by the configurations of state interests and the distribution of state power" [72]. History repeatedly shows that large powers often transgress international law when it serves their national interests. Yet studies show that violations of law can hurt the interests of the transgressors even when they seemingly get away with it. One example is the United States' failure to meet its obligations to destroy chemical weapons under the 1993 Chemical Weapons Convention, which has weakened efforts to pressure other parties to destroy their own munitions [73].

deflect the attention of domestic or foreign publics from the coercive pursuit of material interests, which could violate the very standards of behavior that the leaders invoked (hence the talk's cheapness) [72, pages 178–9]. The theory helps to explain Western rhetoric in other domains of conflict. In 2003, George W. Bush referred to legal provisions of the UN Security Council requiring Saddam Hussain to dismantle weapons of mass destruction and Tony Blair invoked the self-defense principle to protect his country against their implied threat, while, on the ideological plane, both leaders appealed to ideals of democracy expansion—all in order to secure payoffs of cooperation and avoid costs of dissensus with other states, especially democratic partners whose security and economic interests did not align with the two leaders' planned invasion of Iraq. The rhetoric of legal obligations and democratic virtues reflected the true views of many Americans and British people (if not also of Bush and Blair). Moral imperatives did not, however, drive the military adventure or its subsequent resistance by much of the international community.

Despite its success in other conflict domains, the cheap talk model does not go far in accounting for Western attitudes in the cyber domain. Adherence to law and norms is not merely a verbal device of rational actors pursuing their preferences in situations of multiple equilibria. Weighing the option of punitive cyber strikes against North Korean computers in the aftermath of the Sony Pictures hack, James Clapper faced the anxieties of legal advisors (because the attacks could have crossed other countries' networks). "The lawyers went nuts," he revealed, "so we didn't do anything on the cyber front. We ended sanctioning a bunch of North Korean generals [76]." "Everything we did at U.S. Cyber Command was subject to legal commitments," affirmed Corn. "I saw this in practice multiple times. International law plays the tempering role that it ought to play. Responses to cyberattacks have to remain calibrated so that they don't infringe upon international law."[12]

One might expect former senior officials to hew to law and norms. But the apparent self-restraint in practice attests to the commitment's sincerity, especially because it seemed sometimes to override security concerns. Some states pursue cyber legalism as an end in itself. For how else to explain the high material costs of obedience to legal ideals that adversaries repeatedly flout? In open adherence to international law, the United States has shown restraint in the destructive use of cyberweapons even when tactical or strategic considerations supported it. In 2003, the Bush Administration decided not to attack the financial system of Iraq in the lead up to that country's invasion [77]. In 2011, Obama reportedly eschewed the use of destructive cyberattacks against the communications infrastructure of Libya in the lead up to NATO's airstrikes against the country [78]. In the few known instances in which the United States and its allies carried out destructive cyberattacks, their purpose was largely conservative: to support the international order by imposing costs on defiers against it, such as the targeting of the Natanz nuclear facility to degrade Iran's suspected nuclear weapons program or the disruption of Islamic State's communications infrastructure to curtail the terrorist group's online publicity efforts [79]. The legal restraints in these and other cases seem to have involved considerations of both *jus ad bellum*, the question of whether sufficient cause exists to justify an act of aggression (the condition of necessity), and *jus in bello*, whether the action's effects are legal regardless of its justness or not (the requirements of proportionality and distinction).

And what of Stuxnet, was it a breach of international law? The answer hinges partly on whether the operation's effects amounted to a use of force. Let us concede to the cheap talkers that it met this criterion. Even so, the operation stands out as restrained when compared with the common actions of the large norm transgressors. It was highly customized to disrupt only the machine complex at the Natanz nuclear facility. Although it infected computer systems in many countries, its payload affected only that one. Compare it with the Russian NotPetya malware, which disrupted infrastructure and affected economic interests in a cascade of industries and countries. And then there is Stuxnet's purpose: to arrest the suspected development of nuclear weapons by a nation prohibited by treaty from obtaining them, whose authorities occasionally obstructed the inspectors of the International Atomic Energy Agency and had expressed a hostile attitude towards the operation's coauthors, the United States and Israel, thereby possibly providing grounds for offensive action under the principle of anticipatory self-defense. Most important, the virtual, nonlethal method of attack meant that it was far less destructive than the alternative on the table—an airstrike—which the Israeli government reportedly preferred [80, 81]. Overall, what stands out about the Stuxnet operation is not that it was the closest example of a use of force in the cyber domain, but that despite its potency it manifested offensive restraint by its narrow targeting and by its replacement of an armed attack.[13]

The motivations of Western nations' vocal commitment to international law are both domestic and international. They are domestic insofar as they reflect the imperative of elected officials to cultivate the perception among their public that they abide by law and norms. Infraction of international agreements and defiance of established ethical standards are not behaviors that a liberal democratic public will commonly excuse except in circumstances of "extreme emergency," such as Churchill's decision to scorch with fire Dresden and other German cities during the Second World War [83]. The point holds even if one accepts that democratic governments will deceive their own citizens about the legality of foreign policy conduct. Consider the Nixon Administration's concealment of the bombing of Cambodia during the Vietnam War, an action whose legality was broadly challenged and which invoked impassioned rebukes even among the president's supporters. The motivation behind law adherence (or its perception) is also international: to violate law and norms blatantly is to undermine the coherence of *all* law in a jungle of sovereign states whose tendencies for violence and chaos officials want to tame with an arsenal of rules, norms, and institutions to enforce them.

Cyber legalism in brief represents a true, if often tested commitment of the United States and other Western nations to uphold the constraints of international law and norms as they might apply in the realm of unpeace. Cyber activity's vague status within international law and its possibly norm-violating nature (from a Western perspective) explain why these nations protest acts of unpeace directed against them, while they themselves rarely carry them out. It is possible that Western nations conduct more damaging cyberattacks than the empirical record reveals. But that is not likely, because acts of unpeace by definition produce social, political, or economic harm that is difficult to conceal from public scrutiny.

Adherence to law (or one's perception of it) limits the design and application of security doctrine. Whatever dimension of doctrine one considers, declaratory or operational, it must conform with the values of the organized society—even if the crudities of anarchic politics mean that law often exists in a state of tension with power and inter-

12 Interview with Corn.

13 The United States has been active elsewhere in cyberspace. For example, the so-called Equation Group, a governmental actor that has been active for almost 20 years, reportedly infected more than 500 computers in at least 42 countries [82].

ests. As Samuel Huntington explained in relation to US defense policy: "Inevitably, the [government] Administration must legitimate its action by invoking general values which command broad support" [84, page 250]. What may seem like policymakers' insignificant attention to the semantics and phraseology of law is a means to secure the legitimacy and endorsement of policy. That does not always mean that lawfulness supersedes security or negates the use of disciplined coercion to achieve it. Rather, the pining for rules and norms and the flashes of raw power are two aspects of the same doctrinal ethos; they cannot be separated into distinct paradigms. Even the warrior is moved by a cause that (by his lights) benefits the world. Even the worldliest diplomat is tempted to brandish the sword to realize a harmonious ideal. It was said of John Foster Dulles that he flashed the Bible in one hand and the nuclear bomb in the other. The parody of the quip applies as much to the statesman as to his whole nation's style of statecraft. As an ideational enterprise, cyber legalism is inward looking. A liberal vision of international affairs underpins it. It reflects the basic necessity of a national psychology that judges itself and the world according to intentions more than actions or capabilities. As Nakasone and Sulmeyer tellingly put it: "[W]e are protecting U.S. interests from cyber threats and staying true to the nation's core values" [58].

Two Universalisms in a Fragmented World

Having reviewed the roots of cyber legalism, let us delve into its workings and limitations more closely. It is a universal doctrine in two key respects. One is its presumption of *universal acceptance*: international law and norms appeal to all members of the international community; where transgression occurs, it is more the result of misperception or the distortions of dictators than of inconsistent values among peoples. To be sure, ambiguity and disagreement exist between states regarding the precise interpretation of law and norms in given contexts [85]. "There is no international consensus on a precise definition of a use of force, in or out of cyberspace," remarked Alexander. "Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force. Thus, whether in the cyber or any other domain, there is always potential disagreement among nations concerning what may amount to a threat or use of force" [54]. But individual states' assertion of their own interpretation of legalities does not erode the supposed deeper consensus on broad principles of interstate conduct. For cyber legalism is not just inward looking; it also looks *outwards* by universalizing the expectation that peoples of other nations—no matter the ruthlessness of their regimes—will also wish to inhabit the imagined liberal utopia. Therefrom stems an important basis for self-restraint in security policy: the desire to sustain at least the perception of abidance of laws (which officials construe expansively) in an effort, internationally, to civilize a jungle marred by dizzying instability and, domestically, to legitimate policy in an emerging realm of conflict.[14]

A second key feature of cyber legalism is the presumption of *universal applicability*: the existing legal framework suffices to restrain conflict in the new (some say revolutionary) arena of cyberspace. Thus, there is no need to create legal principles; rather, one must figure out how to apply old ones in new contexts. The United States' position is that the law governing armed conflict "should regulate the use of cyber tools in hostilities, just as it does other tools" [91, page 4]. The presumption is also conveyed by Mogherini's commitment to "the existing consensus" on international law, a consensus supposedly embodied in multilateral reports of the UNGGE or the OEWG [92, 93]. NATO too reiterated "that international law applies in cyberspace and must be respected," [71] betraying a frustration, easily detectable in Secretary General Jens Stoltenberg's protests against Russian actions, that adversaries neither respect nor apply the law [94].[15]

Are these two universalistic presumptions accurate? Despite protestations that Russia, China, and other nations routinely violate international law and norms in cyberspace—for example, Obama's claim that the DNC hack breached "established international norms of behavior" [95] or Stoltenberg's condemnation of Russia's "blatant attempts to undermine international law and institutions" [94]—the notion of universal appeal is in one sense accurate. Let us not forget that Russia and China publicly accepted the nonbinding recommendations of the 2015 UNGGE report affirming that international law applies to cyberspace [75]. As permanent Security Council members, they participated in all rounds of UNGGE discussion. Indeed, the Russian government was the first to propose, in the late 1990s, the creation of a multilateral forum for the clarification of norms of offensive cyber conduct. Putin has publicly avowed his country's commitment to international law. In 2013, he promoted "the preparation and adoption by the United Nations member states of international legal instruments regulating the application of the principles and rules of international humanitarian law in the use of ICTs" [96]. A Russian representative at the United Nations similarly affirmed in 2020 that "the existing universally recognized norms and principles of international law fixed in the UN Charter are fully and unconditionally applicable to the sphere of information and communication technologies" [97]. None of this is to argue that Russia, a challenger state against the international order, obeys international law for reasons other than the national interest. It is merely to point out that in the view of geopolitical adversaries, established law and norms are acceptable but in a way that does not offer the clear constraints that Western leaders ascribe to them. The framework applies in the positive rather than in the negative: it does not clearly limit acts of unpeace.

The heat of the argument about the law of cyber conflict, therefore, obscures the fact that the main contenders agree on a fundamental point: they all support the application of existing international law to the cyber domain, but for opposite reasons—one side because it wants to use the framework to limit unpeace, the other because the framework enables more than limits it.

The notion of universal applicability is more problematic. Nations differ on the question of the legal framework's relevance to cyber conflict. The Western view might find credence in rulings of the International Court of Justice (ICJ), although they require interpretive creativity. In 1996, the Court stated that the UN Charter provisions defining prohibitions on the use of force, the right of self-defense, and the Security Council's competence to authorize uses of force "apply to any use of force, regardless of the weapons employed." That is, the principles of *jus ad bellum* that define acceptable grounds for the use of weapons among states apply to the regulation of cyberweapons. The court voiced a similar view in relation to *jus in bello* by noting that international humanitarian law applies to new

14 The universality of liberal democratic values is a precept not only of American foreign policy but also of European approaches to international affairs. See [86–90].

15 Corn expressed a similar point: "I don't anticipate that at the GRU or in PLA hacking units there is an analogue of Gary Corn telling the commander that international law says this or that about what we can do. I don't see Russia or China particularly constrained by international law." (Interview with Corn.)

"means and methods" of warfare. This interpretation draws further support from Article 36 of the Additional Protocol I to the Geneva Convention, which requires a review of new means of warfare [98]. Western references to the applicability of international humanitarian law and the law of armed conflict to cyberspace, then, imply a stretching of the logic of the ICJ's rulings to forms of conflict less than war.

The empirical record paints another picture, however. The existence of the punishment puzzle betrays the weakness of the notion of universal applicability. The persistent failure of Western nations to punish activity that their leaders regard as gravely damaging to national security suggests that they struggle to situate the activity within the legal universe. The vast corpus of international law and norms regulating interstate rivalry, ranging from the UN Charter Principles to the law of armed conflict to regional security treaties such as the NATO treaty, centers on the two benchmarks of armed attack, a clearly defined notion denoting significant destruction of physical property and loss of life, and the use of force, a more ambiguous notion that implies physical harm if not necessarily armed attack. This framework does not commonly recognize the right of nations to carry out reprisals outside of those two situations. Yet no cyber action so far has clearly met their criteria. As we saw, it is disputable whether Stuxnet was a use of force; even if it was, the incident remains an outlier event. Tellingly, even the operation's Iranian victims played down its consequences, as expressed by President Mahmoud Ahmadinejad in 2010: "[The attackers] succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts" [99].[16]

And yet a growing number of cyber actions have abused the customary limits of strategic competition in peacetime. It is by now familiar to point out that cyber conflict occurs below the threshold of war. The main interpretive value of the notion of unpeace is to emphasize the possibly more important but less recognized point that much of it also transpires *above* the threshold of peace. For this reason, the term unpeace is analytically more useful than the alternative label "nonwar"; it emphasizes the difficulties of figuring out how to respond to breaches of the peace with peacetime legal devices that do not pack a sufficiently strong punitive punch.

Although not explicitly defined by treaty, statesmen and scholars alike have regarded the notion of peace to mean the absence of acts of war or gross human rights violations (which do not always occur in wartime). This treatment is implied in the language of UN documents referring, for example, to the goal of "restor[ing] peace following the outbreak of armed conflict, and to promote lasting peace in societies emerging from wars" [100]. Similarly, the diplomacy of preventive disarmament focuses on the preservation of peace by reducing small arms in conflict-prone regions; on peacekeeping in the demobilization of troops and the maintenance of ceasefires; and on peacebuilding to establish the social, economic, and institutional conditions that prevent a recurrence of civil war. The UN Security Council resolution specifying the purposes and tasks of the Peacebuilding Commission explicitly references "post-conflict" scenarios that by their nature entail ruinous physical violence and loss of life [101]. These peace-oriented activities are diverse and sometimes only vaguely defined, but they share a central objective: to prevent or eradicate organized political violence.

Political thinkers have supplied a similarly binary understanding of war and peace. Thomas Hobbes famously and darkly described life in the anarchic jungle as a "state of war," not because war is incessant but because it can at any time break out. Hobbes wrote primarily about life in the domestic state of nature; he was less concerned about the international jungle. But some international relations thinkers (particularly realists such as Hans Morgenthau) have applied his concepts to make sense of international relations [102–106]. In a Hobbesian conception, peace is a state in which actors expect and prepare for future war. Relations among coexisting states constantly alternate between a situation in which war is "on" and one in which it is "off."

The absence of violence is not the only defining element of peace. Equally important for our purposes is the notion of peace implied in Hedley Bull's idea of an "international society" (which has affinities to classical realism) in which sovereign states bound by common basic values seek not merely to limit war, especially a generalized war such as the two world wars that threatens an implosion of the states system, but also to keep interstate rivalries within acceptable boundaries so that the units' sovereignty and security are preserved even if war occurs [107].

Also notable is the unforgettable definition of "cyber peace" provided by Secretary-General of the International Telecommunication Union Hamadoun Touré: "a universal order of cyberspace" that features a "wholesome state of tranquillity, the absence of disorder or disturbance and violence" [108]. Ambitious for its allusion to a stable political order among states, the notion is loftier than historical developments have allowed. But it is useful for analysis because it points to a fundamental condition of peace, namely, the existence of regularized interactions among players such that even in the absence of a World Leviathan to punish deviators they can achieve stable expectations of behavior in a competition for security that is tolerable because its aims are limited and its means are familiar.

The existing legal framework captures much of peacetime cyber activity, but chiefly within the narrowly conscribed realm of domestic law (see Fig. 1). Financial fraud or the theft of money via the Internet, such as North Korea's hacking of cryptoasset exchanges in South Korea, are normally proscribed by the domestic penal code of the victim nation. National authorities might struggle to prosecute the culprits if they reside in a foreign jurisdiction, but at least the applicability of law—some law—is clear.

The framework applies most neatly in the realm of war. The absence of cyberwar in the presence of arms to carry it out reveals a rare strength of the international legal order: there has been no cyberwar because it is the easiest form of conflict to address. A scheming attacker knows that it would almost certainly elicit a response commensurate with conventional war. Cyberwar, then, is a realm of conflict in which international law and deterrence doctrine neatly align—hence its absence so far.[17]

Less clear is the case of unpeace: harmful action whose magnitude of physical harm does not rise to the level of war, and whose

16 For the purposes of this analysis, the distinction between an act of war and use of force is inconsequential, because international law recognizes the right to retaliate in both cases.

17 When does a cyber action entail a sufficient cause to invoke a belligerent reprisal? The question is important because the absence of cyberwar does not signify the impotence of modern weapons. Scenario modeling suggests that cyberattacks could inflict severe physical damage on vital infrastructure and thereby produce human deaths. Conceivable examples are easy to find: a cyberattack that kills people by disrupting a city's power supply or by derailing a passenger train; or one that creates an "existential" danger by disabling a nation's nuclear arsenal [109]. These scenarios would implicate the UN Charter principles of a use of force or an armed attack. Harder (and still unresolved almost 10 years after Jack Goldsmith posed it) is the question of when a cyberattack that slowly degrades the functionality of a critical infrastructure amounts to a use of force or war [110, 111].

Legal Categories of Hostile Cyber Activity

Peace	Unpeace	Armed Attack / Use of Force
Examples: • Standalone cyber espionage or reconnaissance • Bulk data collection of foreign targets • Cryptoasset exchange hacking • Financial fraud	Examples: • Large-scale infiltration and surveillance of government networks (e.g. SolarWinds) • Indiscriminate industrial disruption (e.g. NotPetya) • Disruption of public health services (e.g. Wannacry) • Systemwide computer malfunction (e.g. Shamoon) • Financial system manipulation (e.g. Bangladesh Central Bank heist) • Information operations during national elections or referenda • Power grid disruption (e.g. Ukraine 2015) • Physical infrastructure destruction (e.g. Stuxnet) • Large-scale industrial espionage (e.g. Aurora) • National-scale economic convulsion (e.g. Estonia 2007)	Examples: • Fatal cyberattack against hospital systems • Fatal cyberattack against transport systems • Disruption of tactical operations in wartime (e.g. Georgia 2008)
Applicable legal instruments: • 2004 Budapest Convention • Domestic penal code	Applicable legal instruments: • Domestic penal code (e.g. U.S. indictment of PLA officers) • Countermeasures (possibly applicable, if a breach of international law can be established) • "There is no playbook" (Michael Lynton, Sony Pictures CEO)	Applicable legal instruments: • Law of Armed Conflict • UN Charter (e.g. Articles 51 & 2(4)) • Regional security organizations (e.g. NATO)

Figure 1: Legal categories of hostile cyber activity.

instruments therefore do not apply, even as it breaches the acceptable bounds of peacetime competition, whose punitive options thus will fall short of a satisfactory response. Cyber espionage in the form of kompromat operations is perhaps hardest of all to address because the legal framework says almost nothing about espionage. Acts of unpeace create problems of legal interpretation for nations such as the United States that apply a "traditionally high threshold for response to adversary activity [39, page 3]." When it comes to devising an appropriate response, individuals with responsibility to shape it have few guideposts to orient them. In the words of Sony Pictures CEO Michael Lynton: "There is no playbook [112]," an insight that applies as much to government decisionmakers as to industry executives caught in the middle of the spectrum of conflict.

International law allows the use of countermeasures—unilateral actions adopted by one state in response to another's actions—but only if the victim can establish that the other side breached the law (such as the principles of sovereignty or nonintervention [113]). But as we saw, it is often contestable whether such a violation has occurred through cyberspace. Even when countermeasures are allowed because a breach has occurred, international law tightly constrains them. Countermeasures require prior notification, thereby potentially diminishing their tactical effectiveness; cannot be used against non-state actors, limiting their application against proxy agents that

often play an important tactical role in cyber conflict [114]; cannot be applied collectively among allies, reducing the compounding effects of a coordinated response; and cannot be used to deter future aggression (merely to curtail or seek reparations for an ongoing wrongful action) [115, 116]. Countermeasures, then, are an un-proactive, nonpunitive, state-oriented, uncoordinated form of adversary denial. The result is a situation in which international law limits the victim's response more tightly than the attacker's initial move.

Cyber legalism, in sum, constrains Western behavior in two ways: first, because of officials' uncertainty about where and how existing law applies (though apply it must!) to cyber actions that are neither war nor peace; second, because of their desire to sustain at least the perception of law abidance through self-restraint in the enterprise of norm creation.

The approach suffers severe limitations. The liberal worldview on which it draws fails to grasp an essential truth about the world it seeks to shape: the anarchical states system does not tolerate noble adherence to law—obeyance of rules for its own sake. What good is it to live according to the precepts of an ideal society if one's neighbors are intransigent villains? To accept the constraints of international law while others flaunt it is to pay the costs of adversaries' imaginative exploitations. There is in the legalistic paradigm a self-fulfilling righteousness: the greater the adherence to law among nations, the greater the costs of neglecting it—hence the necessity, ultimately, for universalism. But it suffers also a dilemma: if nations stray from the rules they themselves espouse—even as a temporary interruption in the imagined order—because others break them, then the norm proponents risk damaging their own ideal enterprise. The inward project of norm enactment and its attendant self-restraints are a precursor to the outward facing project of norm expansion.

This dilemma seems insoluble under present conditions. Cyber legalism implies a universality that the realities of international politics do not allow but without which the approach cannot succeed. To assert that nations must adhere perfectly to legal and normative obligations implies that nations want or can be persuaded to do so. But the end of legal infringements by sovereign states is neither historically possible nor philosophically desirable.[18] For this scenario requires a perfection in the design of law that cannot be implied and the presence of an impartial enforcer that anarchical politics cannot guarantee. Nations, especially large ones, disagree—sometimes fundamentally—about the legal vagaries of cyber conflict. Adherents of cyber legalism assume that international law limits actions above *and* below (to a point) the level of war and use of force. Adversaries' persistent violation of the undefined lower boundaries suggests that in their view legal constraints apply mainly (possibly only) above the war threshold. They constrain unpeace only weakly; it goes unpunished mainly because it is *unpunishable*.

Gaps in the applicability of international law to cyber conflict mean that much of the effort to strengthen institutional constraints falls into the realm of *lex ferenda*, or future law. The curtailment of intensifying conflict, however, cannot wait for a future that might never arrive. Until and unless the legal system is equipped with instruments to limit technological acts of unpeace, policymakers must find a solution to problems of cyber conflict prevention elsewhere—in the realm of strategies to deter aggression by rational means.

18 The legal doctrine of *clausula rebus sic stantibus* allows the violation of legal obligations when the circumstances underlying an agreement change.

The Logic of Consequences: An Interim Solution

Early cyber norm abiders are condemned to pay the price of transgressors' exploitative maneuvers. The empirical record exposes the failure to address the punishment problem within the current legal framework. Policymakers consistently fail to penalize offensive acts decisively; therefore, they continue unabated. Where is the deterring power of past criminal indictments and targeted financial sanctions [117–120]? Why has persistent engagement—now in its third year of implementation—failed to disarm, disorient, or lure foreign culprits away from prized targets? The gravity of the state of cyber unpeace and the failure to arrest its growth are clear. Western strategic planners have begun to figure out *when* and *how* to use cyberattack as an instrument of foreign and security policy, while continuing to grapple with the reverse side of the puzzle—how to *punish* it when it strikes at home.

The attempt to develop more effective doctrine is hindered by the very legal system that makes it necessary. Old modes of thinking about security and conflict are at the root of Western failure to resolve the challenge of cyber conflict prevention. Because policymakers prioritize legal and diplomatic conventions grounded in traditional notions of armed conflict or physical violations of national territory, they struggle to deal with actions—no matter how politically or economically damaging—that fall below that recognizable threshold. The international rulebook prioritizes war; so too does security doctrine based on a liberal interpretation of it.

What is to be done about this situation? In the absence of adequate legal and normative instruments to stop acts of unpeace, a solution must be found in a consequentialist logic of action, one that appeals to opponents' rational considerations of material interests rather than to a sense of appropriateness that has not yet formed and may never do so. The main objective is calculated deterrence: to convince adversaries that the retaliatory costs of technological aggression are greater than its material gains. Doctrine to be sure must accord with international law, unless one is prepared to pay the legitimacy costs (domestic and international) of transgression. But the costs of transgression are in fact limited, for we established earlier that the expansive reading of international law within cyber legalism is far from universally valid. To transcend its limits is to break not the law, which remains contested, but one's own interpretation of it.

A consequentialist approach has the chief advantage of being immediately executable. It does not require the lengthy process of socialization implied by cyber legalism, which faces numerous time-consuming obstacles, beginning with the question of norm definition, about which nations disagree and on which much interpretive work remains to be done—even if states agree on starting principles—and followed by norm internalization, a complex and lengthy process even when there is consensus on which new norms to institutionalize [24, 121]. Crucially, conjuring a logic of consequences does not require abandoning the normative enterprise; one can still construct norms for a future world, one where law is more than just the law of the jungle. And that is the point: to exact penalties *ex ante* for the violation of norms that one seeks to institutionalize *ex post*. Nor must calculated punishment contradict the norms that one seeks to build. Recall that the question is how to *prevent* acts of unpeace by carrying out, or threatening to carry out, a commensurate response, not when to use unpeace offensively (although daring policymakers may want to explore this question too).

The scope of this article does not allow a full exposition of such doctrinal reforms. What follows is a brief discussion of a possible alternative approach—"punctuated deterrence"—that seeks to address gaps in international law while correcting the internal flaws of

classical deterrence. The strategy departs radically from the classical regime of punishment, which prescribes responses to single incidents. Rather, it seeks to transform the psychological basis of opponents' calculations by punishing a *series* of actions and their *cumulative* effects [14, chapter 7]. Thus, the adversary must calculate the chances of retaliation arising not only from single actions but also from a collection of them—how many actions, against what targets, and which of their aggregated effects. Moreover, the strategy gives the option to retaliate wherever and whenever it fits the victim's interests and capacities. The flexibility for reaction is larger relative to classical deterrence, because the defender can set as it wishes the threshold of aggregate harm calling forth penalties. The many possible permutations of punishable actions and their attendant penalties give the defender a wide scope of maneuver in which to craft a response that keeps the adversary on its toes. The reaction need not be persistent; penalties can be bundled into a single action or a small number of actions. And that is the purpose: to economize offensive resources and civil service capacity by inflicting penalties in a concentrated burst rather than in a series of hits within a broad campaign of persistence. In short, rather than defending forward, punctuated deterrence seeks to *punish backwards*.

Whatever rational approach one pursues, the follies of cyber legalism demand departures in thinking about cyber conflict prevention. Four principles can orient the search for more effective doctrine. First is *the accretional principle:* nations that suffer sustained acts of unpeace should punish them as strategic campaigns rather than as individual actions. Adversaries do not regard their actions as isolated incidents [14, 38]; neither should the victims. The cyberattacks against Estonia's financial systems in 2007, the attacks against Georgia's central bank (and the accompanying military invasion), the series of cyber operations that struck targets in Ukraine after President Viktor Yanukovych's ousting from power in 2014, and related actions were elements of a broad Russian effort to undermine public confidence in the cohesion and security of NATO and the EU or else to raise the costs of accession into them. To say that every offensive move demands a punitive response, however, is not to say that the punishment must issue immediately or singly. A responder can regain the macro initiative by delivering penalties in a concentrated fashion at a time and location and in a manner defined by the victim rather than by the opponent.

Second is *the principle of virtual integrity.* International law as we saw privileges the physical world over the virtual world. The Western conception of cybersecurity reflects this prejudice: it gives more weight to the protection of material infrastructure and geographic territory than to the integrity of information spaces. It is an artifact of a previous era in which the cohesion of the polity relied fundamentally on the inviolability of the national soil. Spies and other foreign agents could affect internal affairs, but nowhere near the extent of influence that is possible with remote, bot-assisted, and algorithmically enhanced maneuvers within modern information spaces.

By contrast, Russian and Chinese conceptions of cybersecurity (if they even call it that) stress "information security" (their preferred term), or efforts to protect the integrity of domestic information flows via the Internet [122, 123]. From this distinction between Western and authoritarian notions of cybersecurity emerges a different understanding also of sovereignty. Russia and China adopt a positivist interpretation grounded in material threats and territorial sanctity—but only to an extent that serves their interests. When Russia denounces as a violation of its sovereignty the financial and other material support that foreign governments give to opposition parties and political figures, or when China protests the United States' failure to accept Chinese territorial claims over Taiwan and the East China Sea, the autocrats invoke the material dimensions of the sovereignty principle. They speak a legal language that many other nations grasp. When these countries affirm cyber sovereignty as a rule of law [75], they mean that the Internet is not a global public good; they will impose full sovereign control upon it. Unspoken is their rampant intrusions upon Western information spaces—for example, to disrupt elections or to steal strategic secrets. Because such actions transpire in virtual rather than in physical space, they are harder to capture within traditional notions of sovereignty protection [124]. As Jack Goldsmith and Alex Loomis observed, "[T]he UN Charter's prohibition on certain uses of force and the customary international-law rule of nonintervention constrains cyber operations by one state in another. The hard question"—the focus of much contention among states today—"is whether international law related to sovereignty prohibits anything more" [125].

Moscow and Beijing in short are quick to invoke the sovereignty principle in the case of *material* intrusions upon their national soil. They invoke the principle to assert sovereign control over the governance of the Internet's physical infrastructure and its data. But they are silent in their own violation of other nations' *virtual* integrity via information operations—a form of sovereignty intrusion that international law does not neatly capture and which therefore could fall within the realm of unpeace.

On this backdrop, the Western security agenda must give greater attention to information security. It is no longer the concern mainly of authoritarian nations whose regimes strive to preserve legitimacy against the grievances of "confused" citizens (as Chinese authorities put it [126]). It is also a legitimate interest of liberal democracies. Its scope must expand beyond the normal concern of stemming illicit activity such as financial fraud and incitement of violence. Containing malicious political and social content deserves security planners' greater attention.

For liberal democracies, however, information security is a severely conscribed practice. They confront a double asymmetry favoring the autocrats. For one thing, on the defensive side, information control does not come naturally to societies that regard freedom of expression as a fundamental right. The operations during the 2016 US election showed that the very openness that defines the democratic political system makes Western nations especially vulnerable to foreign information campaigns. Democratic societies struggle with a fundamental tension that spares autocracies: how to protect the integrity of political discourse without violating freedoms of expression. The challenge of information governance is complicated by the fact that social media platforms are designed, owned, and operated by private companies (e.g. Facebook and Twitter) that are free from the control of government and that may even work against its interests. The need to involve them at the center of regulatory efforts is another hurdle that autocracies do not face. Yet private sector interests will not always align with those of the government, as demonstrated in the Apple–FBI contention following the San Bernardino terrorist attack in 2015.

For another, on the offensive side, Western nations have less opportunities to operate effectively within adversaries' information spaces. Closed political systems enjoy levers of information control that can stamp out the expression of dissent but which are constitutionally unavailable in a democracy. China operates a vast apparatus of Internet surveillance and censorship (the two go hand in hand) that the authorities routinely use to stanch the flow of ideas that the regime considers subversive [123]. Vladimir Putin's regime has devised a legal framework for Internet surveillance and acquired cen-

soring tools that it often uses to repress political dissent.[19] The autocrats' domestic Internet is not frontierless like democratic networks. Because routers and servers occupy physical space, online communication is readily subject to their jurisdictional control.

Western nations, moreover, do not have a hundred years of doctrinal refinement of information warfare as Russia does. They should develop their own concept and method that governments can employ where opportunities for strategic gain arise or at least to counteract the effects of opponents' maneuvers. Here, the double asymmetry may limit the gains while presenting new dangers. A central challenge is to figure out how to limit foreign intruders' ability to harm the polity's virtual integrity while respecting basic freedoms at home and one's notion of appropriate behavior abroad.

Punctuated deterrence offers punitive options outside of the information space that transcend the plane of contention in which adversaries enjoy a distinct advantage. Punishing information operations to deter the adversaries requires exposing inconsistencies in their stance on sovereignty, which at home asserts sovereign prerogatives of information control, while abroad it allows intrusions upon the information space of other nations. It is a mark of the artfulness of Russian diplomacy that it can operate decisively between these two contradictory policies and succeed at both.

Third is *the principle of issue linkage*. As Henry Kissinger pointed out at the height of the Cold War, linkage is often a reality of diplomacy rather than a choice because of the interdependence among issues [128, pages 125–6]. Issue interdependence is especially pronounced in today's technologically entwined world. Actions in one compartment of cyberspace inevitably affect interests beyond it; possibly they influence issues and regions much further afield. But linkage can also be assertive if it deliberately ties together progress and concessions in separate realms of diplomacy—that is, a move to leverage interests in one realm by affecting them in another.

Punctuated deterrence prescribes a combination of options to inflict costs in multiple realms, not just in the cyber domain. Existing law as we noted limits cyber countermeasures. At any rate, to punish aggression only in kind encourages the view that adversaries can harm interests in a domain in which they enjoy many advantages while avoiding costs where one is superior. The linkage method addresses this imbalance. It encompasses "cross-domain" deterrence, which can involve imposing broad-spectrum (as opposed to narrowly targeted) financial and economic sanctions that affect national or sectoral as opposed to individual or organizational interests; costs in negotiations for a new nuclear arms limitation treaty with Russia; penalties in the commercial relationship with China or in the form of stronger security guarantees for Taiwan, South Korea, and Japan; and so on. Western policy so far has made insufficient use of these punitive devices, especially broad-spectrum sanctions. Sanctions often target individuals or organizations directly involved in the operation; the parent government, industries, and economies are normally spared—but this need not be so.

Fourth is *the principle of declaratory credibility*. Deterrence is at bottom a psychological mechanism: it relies on the attacker's firm belief that the penalty for attack is not worth assuming because it is costlier than the gains and that the penalty will actually ensue following an attack. Two dangers exist here. One is a vague promise of penalties. To state that one might retaliate against cyber actions invites the opponent to consider that one might in fact *not* retaliate. It is important to state plainly, therefore, the intent to retaliate and that one will do so for a series of actions. The unfulfilled promise of penalties presents a second danger. Nothing is more damaging to the psychological edifice of deterrence than to announce punishments that do not materialize. Although the attacker controls the conditions that trigger the penalties, it is the responsibility of the victim to inflict them. Clear diplomatic signaling is thus a crucial aspect of effective deterrence. Signaling must communicate to opponents that for punishment purposes, actions will be decisively treated as a comprehensive set of offensive activity, not as separate moves eliciting isolated penalties.

As the maven of nuclear strategy Thomas Schelling pointed out, declaratory ambiguity about deterrence thresholds can prevent attack if it makes the adversary guess conservatively about the location of the line of response. Declaratory certainty by contrast invites the risks of "up-to-the-line" attack; it can be escalatory up to that line [129]. Western cyber policy suffers the twin follies of both postures: too much ambiguity in identifying the response lines of unpeace, which prompts a liberal interpretation of their location, and too much certainty in defining the "red lines" of cyberwar, which creates the perception that war is the ultimate—perhaps only—form of aggression to which deterrence policy applies.

The Necessity for New Strategy

The defining feature of an anarchic political system is not peace but order. In this regard, the international cyber domain is not just an unpeaceful but also a pre-anarchic environment: it lacks stable expectations of behavior among sovereign contenders. Policymakers and analysts have yet to develop the institutional conditions of orderliness that make security competition in other conflict domains largely bearable because it is regularized and because clear rules and expectations of behavior guide the rivals [53, 130].

For all the assertions that international law applies to the regulation of cyber conflict, dissonances among states reveal the failure of the legal and normative framework to curtail it. To Western nations, the framework is relevant because it constrains behavior: it allows them to chart a course towards an imagined orderly universe they want to inhabit even as they still lay down its institutional foundations. To adversaries such as Russia and China, the legal framework is relevant for the opposite reason: it offers few clear limits on a large and expanding range of hostile activity that the autocrats carry out to pursue their interests. To Western officials, international law is a map out of the chaotic international jungle towards a more restrained society. To the autocrats, it is a very different kind of map: it reveals roads inside rather than out of the jungle; it guides movements within a primitive society of only thinly shared ideals and few consequences for violating them.

Therefrom stems a major contradiction in Western cyber strategy: it is both too lenient, because it fails to punish actions that law and norms after all do not clearly limit, and too strict, because an expansive interpretation of the rules curtails one's own scope of offensive maneuver. It struggles to check adversaries' pursuit of strategic gains even as it passes up opportunities to seize them.

Incessant breaches of the peace in the absence of war betray the failure of current Western policy to prevent them. Policy approaches that prioritize a system of law that does not apply neatly and universal norms that do not yet exist—and which one cannot unilaterally wish into existence—reveal the extent to which the problem of

19 Russian government censors have not been as stringent as their Chinese counterparts. Russian residents, for example, enjoy access to Western social media platforms such as Instagram and Twitter, which Beijing bans. Russian information control is more assimilative: it seeks to convince citizens to use native Russian services—or as Andrei Soldatov put it, "to live in a bubble of Russian apps" [127].

repeating conflict is chiefly doctrinal rather than institutional. Institutional solutions possibly lie in wait. But until the legal system is upgraded, unless a new normative consensus emerges, an approach that prioritizes law and norms will feed rather than solve the problem.

Western policy requires new approaches to cyber conflict prevention that emphasize calculations of material interests over the pursuit of ideals. It must fill the gap of law and norms by operating, much like adversaries, in spaces where the existing framework does not recognizably apply—an effort to inhibit boldness with boldness. New punitive strategies such as punctuated deterrence represent a plea to consider the rational and pragmatic benchmark of conflict reduction, not a preachment for liberal ideals that events have ruled out. When so much is at stake, when the very integrity of democratic institutions is in peril, security strategy requires an option to strike back to convince the opponent that rules must be followed even if they are still being written. The grudging—even forced—acceptance of new rules is the first step in the long road to their internalization by opponents who contest them. If one accepts this notion, then several principles of action become clear: the necessity for punishing a series of blows rather than single ones; the expansion of the arc of deterrence to the intangible interests of information security (the nation's "virtual" integrity); the linkage of issues across domains; and above all clarity and firmness in signaling a willingness to strike back.

Future historians can decide whether a new policy course that exacts greater penalties prevents more conflict than it risks. But analysts today can already conclude that the policy of weak response has produced unacceptable results. Resolution of the challenge of cyber conflict prevention demands a degree of sincerity that existing policy does not supply: a commitment to defend national interests and values with credible punishment until future generations have created the institutional conditions for lasting stability. The protection of national security cannot function in the future perfect tense; it calls for solutions (even temporary ones) in the present. Western security doctrine must outgrow the confines of an outmoded legal order that prioritizes the peace–war binary. In the current era of technological conflict, officials cannot afford to indulge in the conceit that old policy dogmas apply where reality negates them. The organization of Western cybersecurity requires new departures in thinking.

Acknowledgments

This publication was supported by The Hague Program for Cyber Norms. The author is grateful to Dennis Broeders, James Shires, Tsvetelina van Benthem, Monica Kaminska, and Jack Kenny for their insightful comments and advice.

Conflict of interest statement. None declared.

References

1. Nakashima E. White House says Sony hack is a serious national security matter and U.S. is weighing a response. *The Washington Post*. https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html. December 18, 2014.
2. Bolton J. *The Room Where It Happened*. New York, NY: Simon and Schuster, 2020.
3. MacAskill E. Hostile states pose "fundamental threat" to Europe, says MI6 chief. *The Guardian*. https://www.theguardian.com/uk-news/2016/dec/08/hostile-states-pose-fundamental-threat-to-europe-says-mi6-chief. December 8, 2016.
4. MacAuley J. France starts probing "massive" hack of emails and documents reported by Macron campaign. *The Washington Post*. May 6, 2017, 2017. https://www.washingtonpost.com/world/macrons-campaign-says-it-has-been-hit-by-massive-hack-of-emails-and-documents/2017/05/05/fc638f18-3020-11e7-a335-fa0ae1940305_story.html.
5. Cerulus L. Von der Leyen calls out China for hitting hospitals with cyberattacks. *POLITICO* June 22 2020.
6. Russett B. *Grasping the Democratic Peace: Principles for a Post-Cold War World* Princeton, N.J. Princeton University Press 1994.
7. Miller G, Nakashima E, Entous A. Obama's secret struggle to punish Russia for Putin's election assault. *The Washington Post* June 23, 2017.
8. Blake A. 'I feel like we sort of choked': Obama's no-drama approach to Russian hacking isn't sitting well. *The Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2017/06/23/the-russia-2016-blame-game-finds-obama/. June 23, 2017.
9. Tait M. The Macron leaks: are they real, and is it Russia? *Lawfare* 2017.
10. Egloff FJ. Public attribution of cyber intrusions. *J Cybersecur* 2020;**6**:tyaa012.
11. Soesanto S. Europe's incertitude in cyberspace. *Lawfare* 2020.
12. Stone J. EU cyber sanctions ID Russian intel, Chinese nationals and a North Korean front company. *CyberScoop* 2020.
13. Stevis-Gridneff M. Recommends limiting, but not banning, Huawei in 5G rollout. *The New York Times*. https://www.nytimes.com/2020/01/29/world/europe/eu-huawei-5g.html. January 29, 2020.
14. Kello L. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.
15. Jacobs B. John McCain says US has no strategy to deal with Russian cyber warfare. *The Guardian*. http://www.theguardian.com/us-news/2017/jan/27/john-mccain-says-us-has-no-strategy-to-deal-with-russian-cyber-warfare. January 27, 2017.
16. Coats DR. Worldwide threat assessment of the US intelligence community. Senate Select Committee on Intelligence. 2019.
17. Nakashima E. US Cyber Command operation disrupted internet access of Russian troll factory on day of 2018 midterms. *The Washington Post*. 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. February 27, 2019.
18. Impelli M. Colorado representative says SolarWinds hack could be "cyber equivalent of pearl harbor." *Newsweek*, December 18, 2020.
19. Perlroth N, Sanger DE. Iranian hackers target trump campaign as threats to 2020 mount. *The New York Times*. https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html. October 4, 2019.
20. Warrell H. SolarWinds and Microsoft hacks spark debate over western retaliation. *The Financial Times*. https://www.ft.com/content/0548b0fb-4dce-4b9e-ab4b-4fac2f5ec111. March 12, 2021.
21. Kaminska M. Restraint under conditions of uncertainty: why the United States tolerates cyberattacks. *J Cybersecur* 2021;**7**:tyab008.
22. Schmitt MN (ed). *Tallinn Manual on The International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
23. Schmitt MN (ed). *Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
24. Finnemore M, Hollis DB. Constructing norms for global cybersecurity. *Am J Int Law* 2016;**110**:425–79.
25. Roguski P. Application of international law to cyber operations: a comparative analysis of states' views, *The Hague Program for Cyber Norms policy brief* 2020.
26. Delerue F. *Cyber Operations and International Law*. Cambridge: Cambridge University Press, 2020.
27. Johnston AI. Thinking about strategic culture. *Int Secur* 1995;**19**:32–64.
28. Singer JD. Man and world politics: the psycho-cultural interface. *J Soc Issues* 1968;**24**:127–56.
29. Fearon JD, Laitin DD. Ethnicity, insurgency, and civil war. *Am Polit Sci Rev* 2003;**97**:75–90.
30. Sanín FG, Wood EJ. Ideology in civil war: instrumental adoption and beyond. *J Peace Res* 2014;**51**:213–26.

31. Johnson DDP, Toft MD. Grounds for war: the evolution of territorial conflict. *Int Secur* 2014;**38**:7–38.
32. Cederman L-E, Vogt M. Dynamics and logics of civil war. *J Conflict Resolut* 2017;**61**:1992–2016.
33. Walter BF. The new new civil wars. *Annu Rev Polit Sci* 2017;**20**: 469–86.
34. Valeriano B, Maness RC. The coming cyberpeace. *Foreign Affairs* 2015.
35. Hollis DB. Re-thinking the boundaries of law in cyberspace: a duty to hack?In: *Cyber War: Law and Ethics for Virtual Conflicts*. Oxford: Oxford University Press, 2015.
36. Rovner J. The intelligence contest in cyberspace. *Lawfare* 2020.
37. Shires J. The simulation of scandal: hack-and-leak operations, the Gulf states, and U.S. politics. *Texas Nat Security Rev* 2020;**3**:10–29.
38. Harknett RJ, Smeets M. Cyber campaigns and strategic outcomes. *J Strateg Stud* 2020:1–34.
39. Achieve and maintain cyberspace superiority: command vision for US Cyber Command. U.S. Cyber Command. 2018.
40. Reichborn-Kjennerud E, Cullen P. *What Is Hybrid Warfare?* Norwegian Institute of International Affairs (NUPI), 2016.
41. Chivvis CS. Hybrid war: Russian contemporary political warfare. *Bull At Sci* 2017;**73**:316–21.
42. Trenin D. Avoiding U.S.-Russia military escalation during the hybrid war. Carnegie Endowment for International Peace. 2008.
43. Barroso J, Fallin M, Foxx V. Republican platform 2016. 2016.
44. Raymond M. Managing decentralized cyber governance: the responsibility to troubleshoot. *Strategic Studies Quarterly* 2016;**10**:123–49.
45. Raymond M. Engaging security and intelligence practitioners in the emerging cyber regime complex. *The Cyber Defense Review* 2016;**1**:81–94.
46. Brantly AF. The most governed ungoverned space: legal and policy constraints on military operations in cyberspace. *SAIS Rev Int Aff* 2016;**26**:29–39.
47. Grigsby A. The end of cyber norms. *Survival* 2017;**59**:109–22.
48. Finnemore M, Hollis DB. Constructing norms for global cybersecurity. *Am J Int Law* 2016;**110**:425–79.
49. Kello L. The meaning of the cyber revolution: perils to theory and statecraft. *Int Secur* 2013;**38**:7–40.
50. Weber V. The worldwide web of Chinese and Russian information controls. Oxford University Centre for Technology and Global Affairs, 2019.
51. DeNardis L. *Protocol Politics: The Globalization of Internet Governance*. MIT Press, 2009.
52. DeNardis L, Raymond M. Thinking clearly about multistakeholder internet governance. In: *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013*, 2013.
53. Kello L. Cyber security: gridlock and innovation. In: Hale T, Held D (eds). *Beyond Gridlock*. Cambridge: Polity, 2017.
54. Advance questions for lieutenant general Keith Alexander, USA Nominee for Commander, United States Cyber Command. 2010.
55. Operational law handbook, chapter 5, Standing Rules of Engagement (Instr. 3121.01B). 2015.
56. Schmitt MN. International law in cyberspace: the Koh speech and Tallinn Manual juxtaposed. *Harv Int Law J* 2012;**54**:25.
57. Michaels J. Hagel encourages restraint in cyber warfare. *USA Today* 2014.
58. Nakasone PM, Sulmeyer M. How to compete in cyberspace. *Foreign Affairs* 2020.
59. Pillars of the international strategy for cyberspace. 2009. https://2009-2017.state.gov/s/cyberissues/strategy/index.htm.
60. University Stanford. Christopher Painter (web profile). https://cisac.fsi.stanford.edu/people/christopher-painter.
61. Broeders D, Cristiano F. Cyber norms and the United Nations: between strategic ambiguity and rules of the road. Italian Institute for International Political Studies 2020.
62. Broeders D. Mutually assured diplomacy: governance, 'unpeace' and diplomacy in cyberspace. Observer Research Foundation 2019.
63. Broeders D, Boeke S. The demilitarisation of cyber conflict. *Survival* 2018;**60**:73–90.
64. Kello L. Private sector cyber weapons: an adequate response to the sovereignty gap?In: Zegart A, Lin H (eds), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Brookings Institution, 2019.
65. Healey J. The implications of persistent (and permanent) engagement in cyberspace. *J Cybersecur* 2019;**5**:tyz008.
66. Harknett RJ. Persistent engagement and cost imposition: distinguishing between cause and effect. *Lawfare* 2020.
67. Evans A. Our shared commitment to law, norms and confidence building in cyberspace. HM Government, 2019.
68. Cabinet Office. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: HM Government, 2010.
69. Manners I. Normative power Europe: a contradiction in terms? *J Common Mark Stud* 2002;**40**:235–58.
70. Moret E, Pawlak P. The EU cyber diplomacy toolbox: towards a cyber sanctions regime? European Union Institute for Security Studies. July 2017.
71. Statement by the North Atlantic Council concerning malicious cyber activities. NATO. 2020.
72. Goldsmith JL, Posner EA. *The Limits of International Law*. Oxford: Oxford University Press, 2007.
73. Koplow DA. Indisputable violations: what happens when the United States unambiguously breaches a treaty. *Fletcher Forum World Aff* 2013;**53**:23.
74. Buchan R. Cyber attacks: unlawful uses of force or prohibited interventions? *J Confl Secur Law* 2012;**17**:211–27.
75. Broeders D, Adamson L, Creemers R. A coalition of the unwilling? Chinese and Russian perspectives on cyberspace. *The Hague Program for Cyber Norms Policy Brief* 2019.
76. Waterman S. Clapper: U.S. shelved "hack backs" due to counterattack fears. *CyberScoop* 2017.
77. Markoff J, Shanker T. Halted '03 Iraq plan illustrates U.S. fear of cyberwar risk. *The New York Times*. https://www.nytimes.com/2009/08/02/us/politics/02cyber.html. August 1, 2009.
78. Schmitt E, Shanker T. US Debated cyberwarfare in attack plan on Libya. *The New York Times*. https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html. October 17, 2011.
79. Bennett C. Pentagon hits ISIS with "cyber bombs" in full-scale online campaign. *The Hill*. https://thehill.com/policy/cybersecurity/277493-pentagon-targets-isis-with-first-full-scale-cyber-campaign. April 25, 2016.
80. Liff AP. Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *J Strateg Stud* 2012;**35**:401–28.
81. Sanger DE. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York, NY: Penguin Random House, 2013.
82. Equation Group: questions and answers, version 1.5. Kaspersky 2015
83. Walzer M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: NY: Basic Books, 1977.
84. Huntington SP. *The Common Defense: Strategic Programs in National Politics*. New York, NY: Columbia University Press, 1961.
85. Lotriont C. Reconsidering the consequences for state-sponsored hostile cyber operations under international law. *Cyber Defense Review* 2018;**3**:73–114.
86. Fukuyama F. *The End of History and the Last Man*. New York, NY: Simon and Schuster, 2006.
87. Gamble A. The western ideology 1. *Govt Opp* 2009;**44**:1–19.
88. Huntington SP. *The Clash of Civilizations and the Remaking of World Order*. New York, NY: Simon and Schuster, 2011.
89. Ikenberry GJ. The end of liberal international order? *Int Aff* 2018;**94**:7–23.
90. Faust J. *Liberal Democracy as Universal Value*. Deutsches Institut für Entwicklungspolitik, 2013:3.
91. Koh HH. International law in cyberspace. *Harv Int Law J* 2012;**54**: 12.
92. Mogherini F. Declaration by the High Representative on Behalf of the EU on Respect for the Rules-Based Order in Cyberspace. European Council. 2019.

93. *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*. United Nations General Assembly, 2021.
94. Stoltenberg J. Statement by NATO secretary general Jens Stoltenberg on Russian cyber attacks. NATO 2018.
95. Obama BH. Statement by the president on actions in response to Russian malicious cyber activity and harassment. The White House, 2016.
96. Putin V. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013.
97. Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (unofficial translation). Carnegie Endowment for International Peace 2020.
98. Biller JT, Schmitt MN. Classification of cyber capabilities and operations as weapons, means, or methods of warfare. *Int Law Stud* 2019;**95**:48.
99. Clayton M. Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program. *Christian Science Monitor* November 30 2010.
100. Peace and security. United Nations (April 1, 2021 last accessed), https://www.un.org/en/global-issues/peace-and-security.
101. UN Resolution 1645. 2005.
102. Morgenthau H. *Politics Among Nations*. Boston: Knopf, 1948.
103. Heller MA. The use and abuse of Hobbes: the state of nature in international relations. *Polity* 1980;**13**:21–32.
104. Bull H. Hobbes and the international anarchy. *Soc Res* 1981;**48**: 717–38.
105. Michael CW. Hobbes and international relations: a reconsideration. *Int Organ* 1996;**50**:213–36.
106. Donnelly J. *Realism and International Relations*. Cambridge: Cambridge University Press, 2000.
107. Bull H. *The Anarchical Society: A Study of Order in World Politics*. London: Macmillan, 1977.
108. Touré HI. The quest for cyber peace. International Telecommunication Union. 2011.
109. Resilient military systems and the advanced cyber threat. U.S. Department of Defense, Defense Science Board 2013.
110. Schmitt MN. Computer network attack and the use of force in international law: thoughts on a normative framework. *Colum J Transnat'l L* 1998;**37**:885.
111. Goldsmith JL. How cyber changes the laws of war. *Eur J Int Law* 2013;**24**:129–38.
112. Cieply M, Barnes B. Sony cyberattack, first a nuisance, swiftly grew into a firestorm. *The New York Times*. https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html. December 30, 2014.
113. Barela SJ. Cross-border cyber ops to erode legitimacy: an act of coercion. *Just Security* 2017.
114. Buchanan B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.
115. Corn G, Jensen ET. *The Use of Force and Cyber Countermeasures*. Rochester, NY: Social Science Research Network, 2018.
116. Deeks A. Defend forward and cyber countermeasures. *Lawfare* 2020.
117. Grand jury indicts 12 Russian intelligence officers for hacking offenses related to the 2016 election. US Department of Justice, Office of Public Affairs. 2018.
118. Grand jury indicts thirteen Russian individuals and three Russian companies for scheme to interfere in the United States political system. US Department of Justice, Office of Public Affairs. 2018.
119. U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. US Department of Justice, Office of Public Affairs. 2014.
120. U.S. charges Russian GRU officers with international hacking and related influence and disinformation operations. US Department of Justice, Office of Public Affairs. 2018.
121. March JG, Olsen JP. The logic of appropriateness. *ARENA Working Papers* 2004;**4**:28.
122. Andrei S, Borogan I. *The Red Web: The Kremlin's Wars on the Internet*. PublicAffairs, 2015.
123. Segal A. When China rules the web. *Foreign Affairs* 2019.
124. Broeders D. The (Im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment. *J Cyber Policy* 2021:1–21.
125. Goldsmith JL, Loomis A. "Defend forward" and sovereignty. *Lawfare* 2021.
126. Li J. China wants regular citizens to monitor online comments for "harmful" history. *Quartz* 2021.
127. Troianovski A. China censors the internet, so why doesn't Russia? *The New York Times* https://www.nytimes.com/2021/02/21/world/europe/russia-internet-censorship.html. February 21, 2021.
128. Kissinger HA. *The White House Years* New York: Simon & Schuster. 2011.
129. Schelling TC. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1963.
130. Kello L. The virtual weapon: dilemmas and future scenarios. *Politique étrangère* 2015;**79**.