



# Ransomware as a Predator: Modelling the Systemic Risk to Prey

LOUISE AXON, ARNAU EROLA, IOANNIS AGRAFIOTIS, GANBAYAR UUGANBAYAR, MICHAEL GOLDSMITH, and SADIE CREESE, Department of Computer Science, University of Oxford, UK

The accelerated pace with which companies, governments, and institutions embrace digital transformation is creating opportunities for economic prosperity, but also increases the threat landscape. Recent orchestrated cyber-attacks have revealed the unpredictability of the harm they can cause in our society, rendering the creation of new models that capture systemic risk more critical than ever. In this article, we model the behaviour of one of the most prominent cyber-attacks: ransomware; in particular, ransomware that propagates between organisations via the Internet. We draw concepts from epidemiological models of viral propagation to reason about policies that can reduce the systemic cyber-risk to the community. To achieve this, we present a compartment-based epidemiological model of predator-prey interactions and run simulations to validate the importance of defensive controls that reduce the propagation of ransomware. Our model suggests that with specific defensive controls in place, other response policies may also become more effective. A prey policy to not pay the ransom may improve the ability of the victim population to recover; while information-sharing may reduce the number of organisations compromised if certain conditions on the speed of threat-intelligence sharing practices are met. These results indicate the validity of the approach, which we believe could be extended to explore the impacts of a broad range of attacker and defender behaviours and characteristics of the digital environment on systemic risk.

CCS Concepts: • **Security and privacy** → **Malware and its mitigation**; • **Computing methodologies** → **Agent / discrete models**; • **Networks** → **Network simulations**;

Additional Key Words and Phrases: Cyber-attacks, ransomware, systemic risk, predator-prey modelling, compartment-based modelling

## ACM Reference format:

Louise Axon, Arnau Erola, Ioannis Agrafiotis, Ganbayar Uuganbayar, Michael Goldsmith, and Sadie Creese. 2023. Ransomware as a Predator: Modelling the Systemic Risk to Prey. *Digit. Threat. Res. Pract.* 4, 4, Article 55 (October 2023), 38 pages. <https://doi.org/10.1145/3579648>

## 1 INTRODUCTION

Cybersecurity harm can propagate through systems, affecting groups of organisations and potentially affect whole economies. Expert communities have been warning about systemic risk from cybersecurity attacks for a number of years, and a recent series of widely impactful cybersecurity events have demonstrated this clearly. The World Economic Forum defines systemic cybersecurity risk as follows: “*Systemic risk refers to the possibility that a single event or development may trigger widespread failures and negative impacts spanning multiple organizations,*

This research was sponsored by AXIS Insurance Company, whose support is gratefully acknowledged.

Authors’ address: L. Axon, A. Erola, I. Agrafiotis, G. Uuganbayar, M. Goldsmith, and S. Creese, Department of Computer Science, University of Oxford, UK; emails: {Louise.Axon, Arnau.Erola, Ioannis.Agrafiotis, Ganbayar.Uuganbayar, Michael.Goldsmith, and Sadie.Creese}@cs.ox.ac.uk.



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs International 4.0 License.

© 2023 Copyright held by the owner/author(s).

2576-5337/2023/10-ART55

<https://doi.org/10.1145/3579648>

*sectors, or nations*” [11]. Key examples are the SolarWinds [4] and Microsoft Exchange [46] supply chain attacks in 2020 and 2021, respectively, which impacted a large number of clients of these technology suppliers, and the WannaCry [70] and NotPetya [76] ransomware attacks of 2017, which spread rapidly between vulnerable organisations. It is anticipated that in the coming years systemic cyber-risk will continue to grow, and systemic events will become increasingly commonplace, as organisations across all sectors become connected to and reliant on the Internet, sharing digital platforms and services [26].

A number of features of the digital environment, resulting from the way it has developed over the past decades, create the potential for systemic cyber-risk:

- **Interconnectivity:** Many systems and devices from a wide range of business and societal applications are connected to and able to communicate with each other over the Internet and are therefore potentially able to propagate malicious code to each other.
- **Lack of diversity:** Dependence on a small pool of technologies and vendors can lead to increased potential for threat and virus propagation; for example, viruses to which a single widely used technology is vulnerable can propagate to impact all organisations using that technology.
- **Interdependence:** As organisations increasingly rely on shared service providers and supply chains, the impact of a failure or breach in one organisation has the potential to cascade through a widening scope of others. Widespread reliance on shared resources (e.g., a small pool of widely used cloud services) creates a concentration of organisations at risk of being impacted simultaneously by a failure of that service.

Given the growing potential for cybersecurity events to have severe, large-scale, and even systemic impacts, it is critical that effective technical solutions, standards, and policies for mitigating systemic risk are developed. To support the development and prioritisation of defensive strategies, there is a need to understand the dynamics of systemic risk: its sources, the ways in which it can propagate, and the effectiveness that various risk controls can have in mitigating it. The ability to understand the effectiveness of defensive strategies against systemic risk is important not only for those designing technical solutions and developing policy, but also for parties assessing the risk exposure of organisations, such as cyber-insurance providers. The ability to account for systemic risk is important for assessing the total risk a single organisation is exposed to and could also support assessment of risk across insurance portfolios (where there may be a risk that multiple systems or organisations will fail simultaneously, for example).

In this article, we explore the utility of compartment-based modelling of predator-prey interactions for reasoning about the effectiveness of defensive strategies against systemic cyber-risk, where we consider systemic risk in terms of the number of organisations negatively impacted by a single event. While we anticipate that the approach could be used to explore a wider range of threats and environmental causes of systemic risk, in this article, we have focused on modelling ransomware that propagates between organisations via the Internet. Our decision to focus on ransomware is informed by the fact that ransomware is prevalent in the threat landscape [6], as well as the potential of ransomware to spread virally, affecting both machines with high levels of connectivity and technologies with dominant market shares, which are key factors in creating systemic risk according to Gorman et al. [35]. The results of a survey conducted in January and February 2022 of 5,600 IT professionals from mid-sized organisations (100–5,000 employees) across 31 countries showed that 66% of organisations had been hit by ransomware in the past year [10]. Furthermore, a joint advisory from the US, UK, and Australian intelligence agencies stated that 14 of the 16 US critical infrastructure sectors were victims of ransomware attacks in 2021, and observed that ransomware attackers were seeking to increase the reach of their impacts, e.g., by targeting the cloud and supply chains [31].

To better understand systemic risk, we present a compartment-based model that can be used to explore the impact of various predator and prey interactions during ransomware attacks (applicable to ransomware attacks in general). To validate its utility, we apply this general ransomware model to a case study: the WannaCry ransomware outbreak of 2017. This is an instance of ransomware that propagated from infected organisations

to other vulnerable organisations (i.e., organisations using the same vulnerable technology) over the Internet. Using this case study, we explore the impact of three defensive strategies on mitigating systemic risk: preventing propagation; information-sharing; and not paying the ransom to gain insights regarding their effectiveness.

In Section 2, we present background on modelling of systemic cybersecurity risk, with particular focus on epidemiological approaches. In Section 3, we summarise the general characteristics of ransomware attacks and defences. These are the characteristics we sought to represent in our compartment-based model for general ransomware, which we present in Section 4. In Section 5, we apply the model to represent the WannaCry case study, and in Section 6, we present the results of running the simulations to explore the effectiveness of the three defensive strategies. We discuss the results in Section 7 and conclude the article in Section 8.

## 2 MODELLING BACKGROUND

### 2.1 Biological Approaches to Systemic Cyber-risk Modelling

A range of models of threat propagation (particularly, computer-virus spread) in computing systems and networks have been presented by researchers previously. Many of these modelling approaches have drawn from biological modelling approaches (research into systemic biological risks predates such research in the cybersecurity field). Researchers have reasoned generally about the applicability of epidemiological models and techniques drawn from nature to interactions in cyberspace [34], including analogies between organisms' individual and collaborative defence mechanisms and cybersecurity defences [25, 53–55, 78].

Prior research has used the biological predator-prey analogy to model interactions between populations of threat actors (predators) and potential victims (prey) (e.g., References [29, 30, 35]). Predator-prey models describe the dynamics of biological systems in which predator and prey species interact and the consequences of these interactions as species compete, evolve, and disperse to sustain their existence. While such models are underpinned by observation of interactions within biological ecosystems, they are valuable for studying attacker-defender dynamics in the cybersecurity arena: the factors that influence population dynamics and the ways in which the actions of one population impact on another.

For examining these cybersecurity dynamics, a number of models have been developed based on epidemiological compartment models [64]. In epidemiology, these models are used to study the spread of infectious diseases among population and include, for example, compartment models for understanding malaria transmission dynamics [51]. Compartment-based models are a specific type of predator-prey model in which the prey are susceptible and the predators are infective. Individuals are categorised according to their infection or symptom status (for example, categorised according to whether they are susceptible to, infected by, or recovered from an infectious disease) [38]. The compartments used in cybersecurity attacker-defender models previously include “susceptible,” “exposed,” “infectious,” “recovered,” “quarantined,” and “vaccinated” [64]. These models can be divided into continuous models (based on differential equations, e.g., References [24, 48]) and discrete models (agent-based models, e.g., References [34, 60]).

Table 1 summarises prior research applying epidemiological models to reasoning about aspects of cybersecurity risk—mainly to modelling the propagation of viruses and in some cases the effectiveness of defensive approaches.

### 2.2 Modelling Approach and Contributions

There is a need for models that can be used to reason about levels of systemic cyber-risk across the wide range of threat motivations and attack types that organisations are exposed to and across the wide range of individual (e.g., strong patching regimes, use of technical controls and incident-response practices) and collaborative (e.g., threat-intelligence sharing) cybersecurity practices that are deployed by organisations. To accurately capture factors causing systemic risk, models need to take into account ecosystem diversity and interdependencies and interconnectivity between organisations. While prior work has explored the impacts of a subset of cybersecurity

Table 1. Epidemiological Modelling Approaches Applied to Systemic Cybersecurity Risk: Research Area, Modelling Approach, and Method

Authors	Research area	Modelling approach	Method
Bose and Shin [16]	Propagation behaviour of malware in mobile devices	Compartment-based epidemiological model	A
Canzani and Pickl [19–21]	Dynamics of disruptive events in interdependent <b>critical infrastructure (CI)</b> systems; impact of attacker and defender interactions	Compartment-based system-dynamics model	A(C)
Chu et al. [24]	Propagation of viruses in computer networks. Explores the effect of time delay caused by the virus's latent period (between nodes being exposed to the virus and becoming infectious) and time delay caused by temporary immunity period (vaccinated nodes lose their immunity after a time when new computer viruses appear)	Compartment-based epidemiological model	M
Din et al. [29]	Propagation of computer viruses; effect of antivirus software (with different parameters including ability to update the signature base) on the spread of infection	Predator-prey model relating number of worms (predators), number of uninfected files (prey), and number of infected files	M
Ding et al. [30]	Propagation of worms. Extends the work of Kumar et al. [48] by incorporating latent delay into the model, to represent latent delay of worms in infected files and investigate the effect of time delay on the system	Predator-prey model relating number of worms (predators), number of uninfected files (prey), and number of infected files	M
Ford et al. [34]	Spread of viruses in computer networks; effectiveness of raising the cost (i.e., risk of “death” through detection) of predation as a defence	Predator-prey model (predators: computer worms; prey: Class 1: infectable node that propagates worms; (2) uninfected node)	A(C)
Gorman et al. [35]	Effectiveness of different levels of diversification of technology as a defensive measure. Found that when a species clusters amongst the more connected vertices in a network it dramatically increases the vulnerability of that network	Predator-prey model (predator: virus; prey: each type of vulnerable device as a distinct species)	A
Gupta and DuVarney [36]	Effectiveness of predator programmes (self-propagating programmes that can clean up systems infected by viruses) of different types (persistent, immunising,...) as a defence against computer viruses	Predator-prey model in which the predators are predator programmes, seeking to remove viruses, and the prey are viruses	A
Jackson and Creese [41]	Propagation of viruses in Bluetooth networks; impact of factors including human behaviours, heterogeneity of devices, and antivirus measures, on the spread of viruses	Compartment-based epidemiological model	A
Kumar et al. [47]	Explores the impact of vaccination and quarantine in reducing the spread of worms	Compartment-based epidemiological model	M
Kumar et al. [48]	Interactions between computer worms, trojan horses, and antivirus software inside a computer system. Impact on number of worms and infected systems	Predator-prey model relating number of worms (predators), number of uninfected files (prey), and number of infected files	M
Nguyen [57]	Propagation of viruses in a totally connected network	Compartment-based epidemiological model	M
Pan and Fung [60]	Malware outbreak within an organisation; effectiveness of incident-response plans (in particular coordinated containment plans) in minimising the impact of the outbreak	Compartment-based epidemiological model	A
Pendegraft [61]	Effectiveness of strategies that reduce value to attackers (e.g., diplomatic efforts or hardening targets to reduce their value). Concluded that defences that reduce the reward to attackers may be superior to those that reduce damage to assets	Ecology-inspired differential equation model describing the relationship between an information system, its users, and a population of attackers	M
Qiang and Lu [63]	Propagation of viruses in computer networks. Illustrate the influence of the configuration of the state-transition diagram on the epidemic threshold	Compartment-based epidemiological model	M
Zhang and Song [79]	Worm propagation; effectiveness of vaccination quarantine as a defensive strategy. Extends the model presented by Kumar et al. [47] by incorporating time delay	Compartment-based epidemiological model	M

M: Mathematical Solution of System Equations; A: Agent-based Simulation (C: Monte Carlo).

defensive practices on threat propagation, the impacts of a number of collaborative practices (such as threat-intelligence sharing) in conjunction with the diverse cybersecurity practices of individual prey have not yet been studied to our knowledge.

While we do not claim to present such a general model for studying systemic cyber-risk, we build on prior work by developing a model capable of representing a three collaborative cybersecurity practices (information sharing, policies against ransom payment, and prevention of propagation), varying levels of cybersecurity practice of individual organisations (such that the outcomes for these classes of organisation as well as for the population as a whole can be studied), and varying attributes of ransomware predators (e.g., their targeting strategies, the ransoms they use, and the propagation behaviours of those ransoms). We envisage that this model could be extended in future work to consider a wider range of attack types, defensive approaches, and systemic-risk factors.

We chose to develop a compartment-based approach to modelling predator-prey interactions, based on the strong applicability of the approach as indicated by the prior research summarised in Table 1. The compartment model allows us to track various relevant states of organisations (prey) in relation to a set of threat actors (predators). Predator-prey dynamics are encompassed in the modelling approach, e.g., we model attractiveness (proximity) of predators to prey, which impacts the likelihood that prey are targeted. The model's outcomes are explored through agent-based simulation, informed by prior work using this approach to explore outcomes of using multiple defensive strategies [41, 60]. We also draw inspiration from prior work in tracking outcomes for the population of predators (as well as for the classes of prey) [29, 30, 48] and in incorporating relevant time delays into the model [30, 79].

### 3 REPRESENTING THE GENERAL CHARACTERISTICS OF RANSOMWARE AND DEFENCE AGAINST RANSOMWARE ATTACKS

We identify the key characteristics of ransomware, and defences against ransomware, that our general ransomware model will need to be capable of representing. Throughout this section, we identify information that leads to specific modelling requirements using labels (e.g., **R1**) that are then referenced in the final subsection where we list the modelling requirements elicited.

#### 3.1 Ransomware: Key Characteristics

Ransomware is a class of malicious software that seeks to inflict damage to victims' systems or data that might be revertible only by the attacker. The attacker uses this damage caused to extort payment from victims, making ransom demands for the restoration of their data, systems, or not releasing the data. Dargahi et al. present a taxonomy of ransomware based on the **Cyber Kill Chain (CKC)** model of cyber intrusions [52], which provides a strong basis for describing the lifecycle of a ransomware attack from an intruder point of view [28].

In our model, we assume that the attacker initially already possesses the ransomware and start from the point at which it delivers the ransomware to selected victims. Therefore, the CKC stages *Reconnaissance* and *Weaponisation* are out of scope for direct representation in the model as actions of the attacker; however, reconnaissance is implied in attackers' selection of victims, and details of ransomware weaponisation inform our representation of ransomware functionalities, as detailed below. The **Command and control (C2)** stage is also out of scope for direct representation in the model; i.e., while our model is capable of representing the resulting attacker and ransomware actions (including ransom demand and payment, sending of decryption keys), the establishment of a C2 channel does not require direct representation. The remaining CKC stages are *Delivery*, *Exploitation*, *Installation*, and *Actions on objectives*.

**3.1.1 Delivery.** At this stage, the ransomware is delivered to one or more victim machines by the attacker (**R2**). Ransomware attackers first need to select the targets they will deliver ransomware to, identified through the Reconnaissance stage. Attackers may be attracted to organisations with different characteristics (e.g., different sectors and revenues), dependent on their motives, and may also be attracted to organisations that use particular technologies (**R1**). Organisation size or revenue, and sector, have both been shown to be factors that may impact attackers' choice of victims. For example, it was observed that "big game" organisations (high-value organisations

or organisations providing critical services) were more frequently targeted in the first half of 2021, after which there was a shift towards more frequent targeting of mid-sized organisations [31]. It was also observed that certain sectors were more frequently targeted by ransomware in 2021, with the Professional and Legal Services industry most frequently targeted [59].

Yuryna et al. found that private sector organisations were more severely affected by ransomware attacks than those in the public sector based on data from 55 UK and US ransomware cases and noted contradictory findings on the impact of organisation size on targeting [77], while Ioanid et al. found that organisation size and revenue were positively correlated with the number of attacks in the case of the WannaCry ransomware attacks [40]. Conversely, Shinde et al. argued, based on questionnaire and interview analysis, that most ransomware uses an untargeted “shotgun” approach [67]. While the relationships between organisations’ characteristics and attackers’ attractedness cannot be easily classified, it is clear that our model needs to be capable of representing targeted (according to the above factors) and untargeted attacks.

There is a variety of vectors by which attackers may seek to deliver ransomware to victim machines. This includes targeting services that are openly exposed to the Internet (e.g., the Remote Desktop Protocol); sending weaponised bundles via email, malvertisement, and delivering them using a USB stick, for example [32].

Some ransomware self-propagates: Once executed on a host, it automatically replicates itself to other machines. It may self-propagate not only within the compromised host’s local network, but also to other IP addresses via the Internet at a speed defined within the ransomware implementation (R9). In some attacks, ransoms have succeeded in self-propagating between hosts multiple times [39], propagating to hosts across a city’s infrastructure [75] and across the world in the case of the NotPetya attack of 2017, for example [76].

**3.1.2 Exploitation.** At this stage, the ransomware exploits a vulnerability to launch itself on the victim machine that it has been delivered to (R4a). This usually means either including a targeted exploit in the weaponised bundle or using an exploit kit [28]. In cases in which ransomware is delivered via an exposed remote service, for example, it might seek to exploit unpatched vulnerabilities in the protocol’s implementation or to carry out brute-force credential attacks. If exploitation is successful, then the ransomware binary accesses the victim machine but has not yet installed its payload.

**3.1.3 Installation.** At this stage, the ransomware executes to install its payload on the victim machine. Some ransomware executes automatically. Other types of ransomware require human interaction to execute (e.g., they require a human to click a link or open a file). There is often a delay between ransomware exploiting a vulnerability on a victim and executing its payload: A FireEye investigation found that from 2017–2019, this delay ranged from 0 to 299 days, with a delay of at least 3 days in over 75% of the cases studied [32] (R5).

Ransomware developers use a range of techniques seeking to deceive, evade, or remain hidden from defensive mechanisms, making detection more difficult. These include traffic encryption and anonymisers and impacting systems slowly and stealthily [28] (R6a).

**3.1.4 Actions on Objectives.** At this stage, the ransomware achieves its intended impacts against the victim. The main objective of ransomware is to achieve impacts that its victims cannot revert, enabling the attacker to extort a ransom payment from them. Ransomware can be designed to take a number of approaches to achieving this, including encrypting, deleting, or exfiltrating data, or locking systems such that users cannot access them [45] (R7).

A significant proportion of (but not all) ransomware encrypts victims’ data. According to Sophos, 66% of 5,600 respondents to their 2022 survey had suffered ransomware attacks in the past year, of which 65% resulted in data encryption [10]. A variety of symmetric and asymmetric encryption approaches may be used, and the difficulty of reversing the encryption varies [14]. Ransomware attackers may seek to establish persistence such that they can further impact prey (e.g., by re-encrypting their files) even after the initial impacts have been fixed [23] (R10).

In some cases, ransomware seeks to remove backups, e.g., shadow copies of files [66], and backup folders [18] (R8). Here, the attacker seeks to prevent the user from recovering their data from backups, leading them to an increased dependence on recovery via ransom payment to the attacker.

After compromising victim machines, the ransomware usually displays a visible message to the machine's user making a ransom demand. This message can take many forms, e.g., impersonating legal authorities [69]. A variety of techniques may be used to pressure victims into paying the ransom [71] (R13), including playing a loud noise [39] or threatening to launch additional attacks [59]. It was reported that in 2021 increasingly diverse approaches were used to pressure victims during extortion, including threatening to publicly release exfiltrated information, disrupt Internet access, and inform victims' partners, shareholders, and suppliers about the incident [31, 65]. In some cases, the ransomware uses wiper elements, threatening to delete data and systems after a time to increase ransom-payment pressure.

While ransomware extortion is genuine in many cases (recovery of data and systems can indeed only be made via the attacker), in some cases the ransomware may display ransom demands falsely (having not succeeded in actually affecting any data or having already irrecoverably deleted the data [22]). In others, the attacker may have no intention of responding to victims' ransom payments by decrypting or unlocking their assets, leaving the victim damaged despite having paid the ransom (R14).

Ransomware attackers may become disincentivised to attack if they do not achieve their aim (receiving ransom payments) for an extended time. Fluctuations have been observed in the activity of ransomware as a result of a failure to gain ransomware payments [59] (R15). For example, a flaw in ransomware used by the BlackMatter (also known as Darkside) meant that victims could recover their files without having to pay the ransom, which led to substantial cost in lost ransomware payments suffered by the perpetrators, whom, it was subsequently observed, went offline [72].

### 3.2 Defence against Ransomware: Key Characteristics

Dargahi et al. describe a defence model against ransomware, relating defence stages to each stage of the CKC. These are in three main categories: "prevent/deny"; "detect/deceive"; "degrade/mitigate ransomware attack's effect" [28]. These categories relate to the five stages of defence described in the **National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)** [58]: Protect, Detect, Identify, Respond, Recover. Similarly, in the below, we consider three stages of defence: preventing delivery, detecting and removing ransomware, and recovering from impacts. Figure 1 shows how these apply to our model of attacker actions and victim countermeasures and states (as well as how our representation of defensive actions maps to the NIST CSF).

Yuryna-Connolly et al. showed that, in a study of 55 organisations hit by ransomware, there was a strong correlation between security posture and attack severity: Organisations with stronger defensive measures were less likely to experience severe impacts as the result of a ransomware attack [77].

**3.2.1 Preventing Delivery and Exploitation (Protective Controls).** Organisations may take a range of actions to protect against the delivery of ransomware. Whether delivery to a victim is successful depends on how well that victim is protected; this may include its email security, access controls, secure firewall configuration, exposure of remote services to the Internet, employees' levels of cybersecurity awareness, physical security, and configurations such as blocking popups and disabling macros, for example [12] (R3). Whether the victim has the necessary vulnerability for the attacker to exploit is dependent on the availability of a patch (R4b) and whether the victim has implemented this patch (R4c).

**3.2.2 Detecting and Removing Ransomware.** The frequent delay between ransomware exploitation and execution means that there is often a window after ransomware's exploitation of a system in which victims have the chance to detect and remove the ransomware before it executes (R6). It was reported that 39% of organisations attacked by ransomware in 2021 stopped the attack before their data could be encrypted [9]. This

suggests that while some organisations are able to detect and remove ransomware binaries before execution, the majority do not.

Some types of ransomware are straightforward to detect, exhibiting overt characteristics that can be picked up relatively reliably by signature-based ransomware-detection tools [39]. Since ransomware developers may include a range of deception and evasion mechanisms, others behave more covertly, with the aim of avoiding detection, and as a consequence may be more difficult to detect unless sophisticated ransomware anomaly-detection approaches are used.

A number of sources give general guidance for organisations compromised by ransomware: Particular actions are generally encouraged or discouraged (**R11**). The key recommended actions for compromised organisations include killing or disabling execution of ransomware binaries; wiping and reinstalling infected devices; restoring from clean backups; and running antivirus software [5, 6, 27]. Disconnecting infected devices from all network connections and the Internet is also recommended by these sources to stop potential propagation within or outside the organisation (**R11c**), and organisations may have additional controls in place such as outgoing firewall rules to prevent propagation (**R9a**); both may be automated through IPS systems.

**3.2.3 Recovering from Impacts.** The key recommended actions for organisations who have successfully cleaned ransomware from their systems are reconnecting systems; restoring data from backups; consulting law enforcement regarding available decryptors; and addressing vulnerabilities and security gaps (e.g., resetting credentials, applying patches upgrading software, and taking other security precautions not previously taken) [27]. Ransom payment is discouraged by most reputable guidance sources and law enforcement (**R11a**): Since there is no guarantee that ransom payment will recover data or systems, and ransom payment does not remove the infection, funds criminal groups, and may make the victim more likely to be targeted again in the future [5, 6, 27].

According to a global study of 15,000 IT professionals by Kaspersky, 56% of victims paid the ransom to restore access to their data or systems in 2020, yet this did not guarantee restoration for 17% of those who paid [43] (**R14**). Similarly, Sophos found that 46% of respondent organisations who were victims of ransomware attacks in 2021 paid the ransom; these organisations got back 61% of their data, on average [10]. 73% of organisations whose data was encrypted stated that they had used backups to restore the data (noting that many respondents used multiple methods to restore the data). Statistics also suggest that victims who pay the ransom are more likely to have their data decrypted than not [2]. We assume that victims are less likely to make further ransom payment to attackers to whom they have previously made payments without receiving the desired response (fixing of impacts) (**R14b**).

Victims may also recover their data or systems by other means, e.g., using decryption tools in the case that the ransomware uses weak cryptography [14, 39] (**R12**). While some ransomware uses sophisticated encryption and is extremely difficult to reverse, not all ransomware is equally effective [65] (**R12a**). An increasing range of decryptor tools are becoming widely available [6, 8]. For example, in the case of the BlackMatter/Darkside failed ransomware campaign, researchers at the cybersecurity firm Emsisoft developed tools to assist victims in recovering their data [59, 72].

**3.2.4 Information Sharing.** Guidance sources recommend that following ransomware attacks organisations share relevant indicators of compromise or lessons learned with security agencies or relevant **Information Sharing and Analysis Centre (ISAC)** [27] (**R11b**). Information-sharing communities may be open-source (allowing anyone who implements the platform, e.g., MISP,<sup>1</sup> to participate), or sector-specific (allowing organisations from the relevant sector to participate) [33] (**R16**). Based on prior work and guidance sources, there is a need to represent five parameters of information sharing that contribute to its effectiveness [62, 68, 74]:

<sup>1</sup><https://www.misp-project.org/>.

- Number of participants in an information-sharing community.
- Timeliness of information sharing: how quickly it is shared on discovery.
- Quality of information shared: incorporates accuracy, completeness, ingestibility of the information.
- Freshness of information shared: how up-to-date the information is. For example, an organisation might take months to discover a compromise and then share information on it immediately. The information would have been shared quickly on discovery (i.e., high timeliness) but would pertain to a months-old threat (low freshness).
- Relevance: how relevant the information is to the organisation. In some cases, information shared may only be relevant to organisations in particular sectors.

In the context of mitigating systemic risk, information sharing is a critical control to explore, since exploiting common vulnerabilities across organisations is a key approach by which attackers can cause widespread compromise. It follows that sharing information on threats related to common vulnerabilities is likely to enable other organisations to mitigate them before they are compromised. In this context, we can assume that the more organisations share information on a particular attack, the higher the priority with which other organisations in the information-sharing community will treat it, since receiving the information from multiple sources indicates a widespread attack.

We can also assume that once the information is known to and shared by a sufficiently high number of organisations, it is likely to become “big news” of which organisations beyond the intelligence-sharing community become aware, e.g., through dissemination of the information through news sources and social media. For example, news about the widespread WannaCry ransomware attack was appearing on Twitter and in news publications throughout the first day of the attack [15, 37].

### 3.3 Resulting Requirements for Representing Ransomware Characteristics, Defence Characteristics, and Information Sharing in the Model

Based on the prior work (particularly Reference [28]), we established the ransomware-attacker lifecycle and possible victim actions in response to attacker actions that our model will need to be capable of representing. These are outlined in Figure 1.

The modelling requirements (the characteristics that the model needs to be capable of representing) are listed below. Throughout Section 4, we reference these requirements to support the selection of the model’s parameters and functions.

- **R1:** Attacker selects target victims that are attractive (through the Reconnaissance stage). The selection may be informed by targets’ revenue, sector, and technologies used, for example.
- **R2:** Attacker attempts to deliver ransomware (with a defined bandwidth) to these targets (i.e., to a defined number of victims in each time window).
- **R3:** Victims’ levels of protection (e.g., through firewalls, email security) may vary. This impacts the likelihood of successful delivery of ransomware by an attacker.
- **R4:** Ransomware seeks to exploit a vulnerability.
  - (a) Ransomware is able to check whether the victim has the vulnerabilities it requires and exploit this vulnerability to infect the victim, if so.
  - (b) Patches for these vulnerabilities may exist in the community, which victims may use to patch their systems.
  - (c) Victims may patch and therefore remove the vulnerabilities required by the ransomware.
- **R5:** A time delay may occur between ransomware infecting a victim and executing on it.
- **R6:** Victims may remove ransomware prior to execution, with probability dependent on the victim’s detection capability and the ransomware’s stealth.

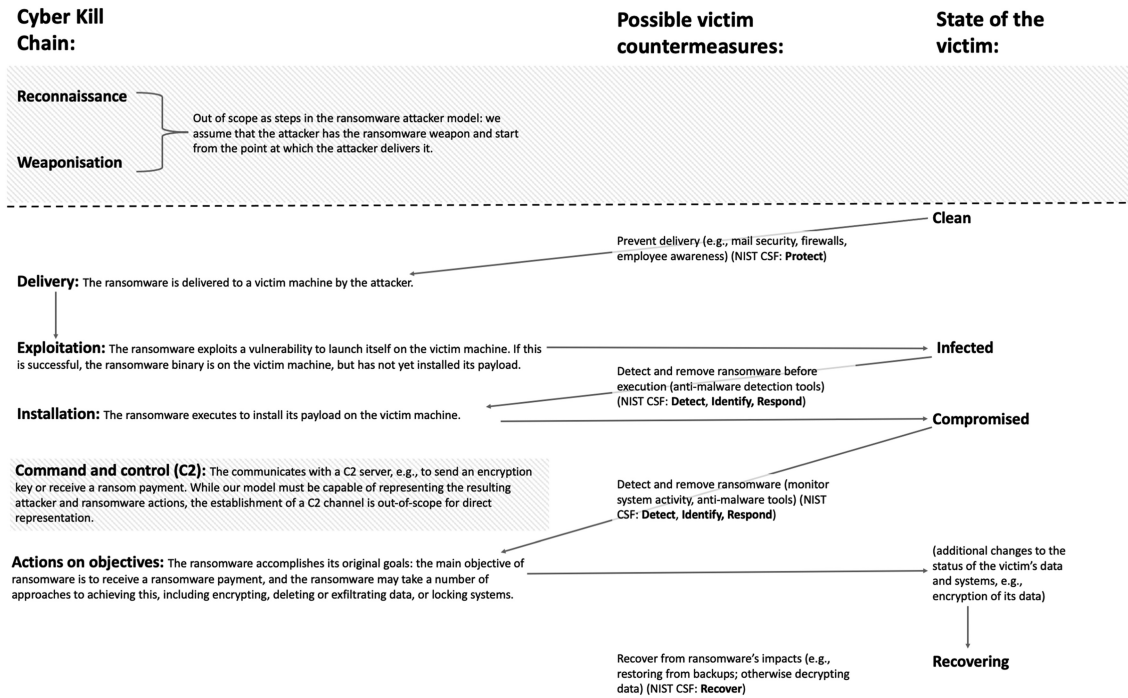


Fig. 1. Overview of ransomware-attacker lifecycle and possible victim response actions.

- (a) Victims' detection capability may vary.
- (b) The difficulty of detecting ransomware (its stealth) may vary.
- **R7:** Executed ransomware achieves its intended impact against victims (which may include encrypting data or locking systems, for example).
- **R8:** Ransomware may degrade victims' recovery mechanisms (e.g., by removing backups, with success dependent on the security of these backups).
- **R9:** Ransomware may self-propagate (with a defined bandwidth) once executed on a host, to infect other hosts.
- (a) Victims may deploy controls that prevent ransomware from propagating to other potential victims.
- **R10:** Ransomware may persist on the victim and repeat its impacts after they have been fixed (e.g., re-encrypt data or re-lock machines).
- **R11:** Victims may take a range of actions in response to compromise by ransomware, as recommended by guidance sources (with probability dependent on their incident-handling capability):
  - (a) Paying the ransom (we represent prey with higher cybersecurity maturity as less likely to pay the ransom, in line with recommended practice)
  - (b) Sharing information on the attack (we represent prey with higher cybersecurity maturity as more likely to share information, in line with recommended practice)
  - (c) Disconnecting infected devices from network connections and the Internet
  - (d) Restoring their data or systems from backups
  - (e) Discarding impacted assets
  - (f) Improving their protective controls and/or patching vulnerabilities
- **R12:** Tools may exist in the community that victims may use to fix the ransomware's impacts (e.g., decrypt encrypted data).

- (a) Difficulty of fixing ransomware's impacts (e.g., hardness of breaking encryption) may vary.
- **R13:** Attackers may pressure victims into paying the ransom (increasing their likelihood of paying).
- **R14:** Attackers may respond to ransom payments by fixing impacts (e.g., decrypting data), with some probability.
- (a) Victims may be less likely to pay ransoms to attackers to whom they have previously made an unsuccessful ransom payment.
- **R15:** Attackers may become inactive as a result of not receiving ransom payments for a threshold length of time.
- **R16:** Information-sharing communities may exist, to which organisations may contribute.
- (a) Organisations from one or more sectors may be assigned to information-sharing communities.
- (b) The quality, relevance, and timeliness of the information that organisations share may vary.
- (c) There is a threshold level of information shared at which the attack becomes "big news," and all organisations may become aware of it.

## 4 GENERAL RANSOMWARE MODEL

### 4.1 Model Overview

The compartment-based model for general ransomware is composed of three types of agents: attackers (predators) that use ransomware, companies (prey) that try to protect their assets, and a world agent that creates events affecting both predators and prey. For each of them, we define parameters, states, and functions in the next sections. Parameters set the characteristics of predators and prey and are used to initiate the simulations and capture the conditions that will allow an action in the simulation to occur or not. States describe the conditions in which each predator or prey can be at a given time, and functions describe transitions from one state to another when specific conditions hold.

### 4.2 Prey

Prey have a set of parameters that describe the characteristics of the organisation, e.g., `SECTOR` (describing the sector), `RESPONSE CAPABILITY` (describing the prey's incident-response capability), and `CONNECTED` (describing whether the prey is connected to the threat vector—e.g., the Internet). Some parameters are constant (they do not change during a simulation, e.g., `SECTOR` and `RESPONSE CAPABILITY`); some are variable (e.g., `CONNECTED`). Full list of constant parameters are described in Table 2, and variable parameters are described in Table 3.

We define classes of prey to represent organisations with similar parameters—e.g., Class A are organisations in `SECTOR` "unregulated," with "high" `REVENUE`, "medium" `RESPONSE CAPABILITY`, and so on. The prey classes are used to model attractiveness to predators, derive the likelihood of prey becoming victims, and determine their response strategies. This can impact the actions of prey and also the likelihood that predators will target them.

Prey agents can be in four states: `CLEAN`, `INFECTED`, `COMPROMISED`, and `RECOVERING`. In the `INFECTED` state, the ransomware has reached the organisation but not yet executed, while in the `COMPROMISED` state, the ransomware has executed on the organisation's systems. In the `RECOVERING` state, the ransomware is no longer running in the organisation, but the organisation has not fully recovered its data. In the initial state, all prey agents are `CLEAN`.

Figure 2(a) shows the prey state machine. Functions define the transitions of prey agents between the four states of the state machine. These functions are called under certain conditions and executed with certain probabilities. A description of these functions and probabilities is provided in Section 4.5.

### 4.3 Predator

The predator parameters describe a number of factors that will be used to describe the behaviour of the predator, the proximity of predator to prey (i.e., the extent to which a predator is attracted to a prey), and the susceptibility

Table 2. Prey Agent Parameters: Constant Parameters

Parameter	Description	Values	Model dynamics	R
SECTOR	The sector of the prey	{Regulated, Unregulated}	Contributes to determining attractiveness of prey to predator (proximity). Predator proximity calculation: checks whether this value matches predator's attraction requirements	<b>R1</b>
REVENUE	The revenue of the prey	{High, Medium, Low}	Contributes to determining proximity (as above)	<b>R1</b>
TECH VULNERABILITIES	The technical vulnerabilities a prey has, making it potentially vulnerable to particular ransomware	e.g., {"eternalblue," ...}	Contributes to determining susceptibility	<b>R4</b>
PROTECTION CAPABILITY	The quality of the prey's protection against ransomware delivery (e.g., firewalls, email security, employee awareness)	{H, M, L}	Probability of successful ransomware delivery is lower for prey with higher PROTECTION CAPABILITY	<b>R3</b>
PATCHING	Quality of patching	{High, Medium, Low, None}	Contributes to determining susceptibility	<b>R4c</b>
DETECTION CAPABILITY	Quality of ransomware detection	{H, M, L}	Probability of removal of ransomware before execution higher if DETECTION CAPABILITY = High	<b>R6</b>
RESPONSE CAPABILITY	Quality of incident response	{H, M, L}	Contributes to determining probabilities of the various responses to compromise	<b>R11</b>
PAYS RANSOMS	Prey's likelihood of paying a ransom in response to compromise	{High, Medium, Low}	Prey with higher likelihood pay the ransom with a higher probability at each step	<b>R11a</b>
SHARES INFORMATION	Whether a prey shares information when they have been attacked	True/False	Prey who share information (True) contribute to the world's intelligence on a ransomware when they are attacked by it. The level of intelligence on a ransomware impacts the likelihood that organisations will remove their vulnerability to it	<b>R11b</b>
PROPAGATION CONTROLS	Whether a prey has controls that prevent onward propagation of ransomware to other prey	True/False	Determines whether ransomware propagates from a compromised prey. If prey has propagation controls, then it does not propagate ransomware when compromised	<b>R9a</b>

**R:** Reference to supporting modelling requirement.

Table 3. Prey Agent Parameters: Variable Parameters

Parameter	Description	Values	Model dynamics	R
CONNECTED	Whether the prey is connected to the threat vector	True/False	A prey can only be attacked and propagate ransomware if it is connected to the threat vector (e.g., Internet)	<b>R11c</b>
IMPACTS	Whether the prey is suffering the impacts of a ransomware attack (e.g., has had its data encrypted)	True/False	A prey becomes impacted following compromise by ransomware and may seek to recover from these impacts by a variety of means	<b>R7</b>
BACKUPS	Whether the prey has backups (which they can use to restore their systems and impacted assets)	{secure, insecure, none}	If a prey has backups, then it can recover their assets from backup with some probability. If these backups are insecure and predator DESTROYS BACKUPS = True, then these backups may be destroyed as part of an attack	<b>R8, R11d</b>
UNSUCCESSFUL RANSOM PAYMENTS	List of the predators that the prey has made an unsuccessful payment to (i.e., the predator did not decrypt/unlock on payment)	[]	Prey are unlikely to make another ransom payment to a predator who has previously not responded to their payment	<b>R14b</b>

R: Reference to supporting modelling requirement.

of prey to the predator. Predators can also be divided into classes based on these parameters. Table 4 contains a description of predator's constant parameters.

Predator agents can be in two states: *ACTIVE* when it is targeting prey or *INACTIVE* when not targeting prey. Figure 2(b) shows the predator state machine. All predators begin in the *ACTIVE* state. If predators do not receive ransom payments, then they eventually become inactive. To model this, we call the predator's *BECOME INACTIVE* function after a defined number of steps have passed without receipt of a ransom payment. A full list of predators' functions is provided in Section 4.5.

#### 4.4 World Agent

There is a "world" agent that performs functions representative of actions taken by the wider community that can make new actions available to individual prey. In particular, these are the creation of patches and tools to fix attack impacts, and controlling the actions of information-sharing communities. Whether an individual prey takes the actions (such as implementing a new patch) made available by the "world" agent is then determined by that prey's characteristics. The parameters of the world agent are presented in Table 5.

**4.4.1 Creation of Patches and Impact-fixing Tools.** The *world* agent creates patches and impact-fixing tools against ransomware with assigned probabilities. If patches and impact-fixing tools exist against a ransomware, then prey may use them to remove their vulnerabilities and fix impacts following an attack.

**4.4.2 Information-sharing Communities.** The world agent also controls the information-sharing communities made up of prey. Based on the modelling requirements presented in Section 3.3 (**R16**), we present our model of

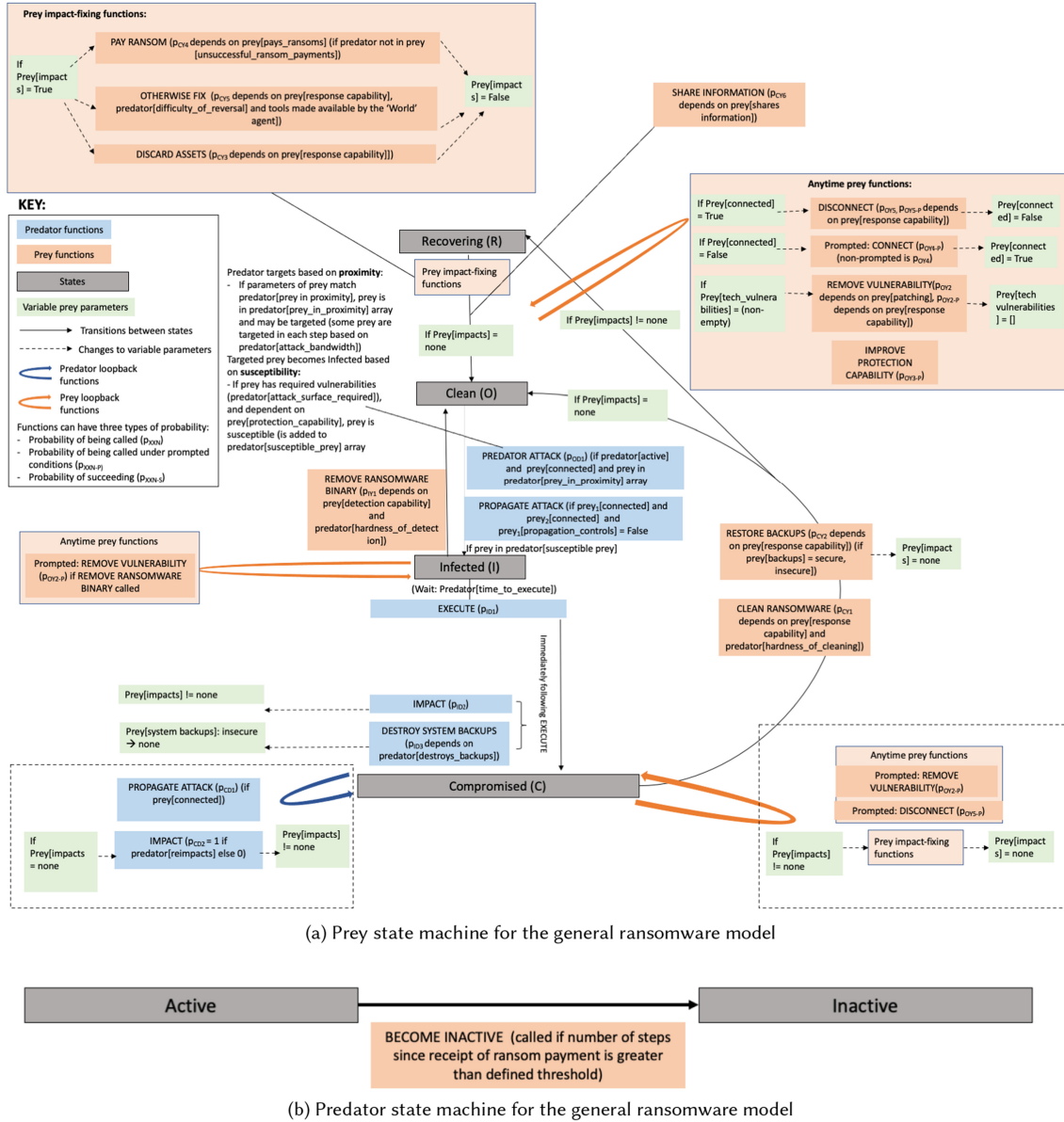


Fig. 2. Depiction of the state machines for all the agents in the ransomware model.

information sharing in Figure 3. As shown, the SHARES INFORMATION parameter (True/False) of prey determines whether a prey that has been attacked shares information on it.

We model two thresholds of INTELLIGENCE LEVEL in the community (R16c). The WORLD agent records the number of prey that have shared information on the ransomware. When the first (lowest) of the two thresholds is reached, the prey that are consumers of threat intelligence (which we assume are the same as the prey that share it, i.e., those for which SHARES INFORMATION is True) are modelled as being in receipt of the information. When the second (higher) threshold is reached, all remaining prey are modelled as being in receipt of the information. This second threshold represents the case where an outbreak becomes “big news.”

Table 4. Predator Agent Parameters

Parameter	Description	Values	Model dynamics	R
ATTACK BANDWIDTH	Defines how many prey per time unit a predator will attack	(number)	At each time unit, each predator targets the defined number of prey	<b>R2</b>
PROXIMITY FACTORS	The factors that affect the predator's "proximity" to prey (i.e., whether the predator is attracted to a prey)	e.g., [SECTOR: regulated, REVENUE: high]	If all elements of a predator's ATTRACTED TO match the parameters of the prey, then the predator is attracted to that prey (the prey is in proximity)	<b>R1</b>
VULNERABILITIES REQUIRED	The prey vulnerabilities the predator seeks to exploit	[]	If all elements of a predator's VULNERABILITIES REQUIRED are in the prey's VULNERABILITIES array, then the predator successfully exploits the vulnerabilities to infect the prey following successful delivery to them (where success of delivery is dependent on the prey's PROTECTION CAPABILITY)	<b>R4a</b>
TIME TO EXECUTE	Defines how long the ransomware takes to execute (once a prey is INFECTED by it)	(units)	After the prey has been in the INFECTED state for the defined time, the ransomware executes	<b>R5</b>
PROPAGATES	Whether the ransomware self-propagates to other prey from a host prey	True/False	If True, then a COMPROMISED prey propagates the attack to randomly selected other prey	<b>R9</b>
PROPAGATION BANDWIDTH	Defines how many prey per time unit the ransomware will attack	(number)	A prey in the COMPROMISED state propagates the attack to other randomly selected prey at the defined rate	<b>R9</b>
REIMPACTS	Whether the ransomware if left on systems reimpacts victims	True/False	If True, then a prey fixes its impacts while still COMPROMISED, and it may be reimpacted	<b>R10</b>
RESPONDS TO PAYMENT	Defines whether a predator decrypts/unlocks a victim's data/systems on payment of the ransom	True/False	If True, then prey's impacts are fixed upon payment to predator; if False, then they are not	<b>R14</b>
PAYMENT PRESSURE	Defines whether a predator pressures prey to pay the ransom (e.g., through threats to expose sensitive data)	True/False	If True, then prey pays the ransom with a higher probability	<b>R14</b>
HARDNESS OF IMPACT FIXING	Defines how hard the impacts of the ransomware are to fix	{high, medium, low}	Impacts on the likelihood that an impact-fixing tool is created by the world agent	<b>R12a</b>
HARDNESS OF DETECTION	How difficult a ransomware binary is to detect (before execution)	{high, medium, low}	Along with prey's ransomware detection capability, impacts on whether it is likely an organisation will detect the ransomware binary before execution	<b>R6a</b>
HARDNESS OF CLEANING	How difficult a ransomware is to clean from the systems after execution	{high, medium, low}	Along with prey's response capability, impacts on whether it is likely an organisation can succeed at cleaning its systems of the executed ransomware	<b>R10</b>
DESTROYS BACKUPS	Defines whether a ransomware destroys backups (with success dependent on the security of these backups)	True/False	If True, then the ransomware destroys insecure backups after execution (PREY[BACKUPS] = "insecure" → PREY[BACKUPS] = "none")	<b>R8</b>
INACTIVE THRESHOLD	Defines the time threshold after which a predator that has not received ransom payments becomes inactive	(units)	After the time threshold has passed without receipt of any ransom payment, the predator becomes inactive	<b>R15</b>

**R:** Reference to supporting modelling requirement.

Table 5. World Agent Parameters

Parameter	Description	Values	Model dynamics	R
PATCHES	The list of vulnerabilities for which the “world” has created patches	$\square$	If a patch exists for a vulnerability, then it is used by prey when they patch	<b>R4b</b>
IMPACT-FIXING TOOLS	The list of ransoms for which the “world” has created impact-fixing tools	$\square$	If an impact-fixing tool exists for a ransomware, then prey may use it to fix impacts in response to compromise	<b>R12</b>
INFORMATION SHARED	The number of prey that have shared information following attack	(units)	When threshold levels of information shared are reached, prey are prompted to take protective actions (as described in the main body of the article)	<b>R16</b>

R: Reference to supporting modelling requirement.

### INFORMATION-SHARING PROCESS

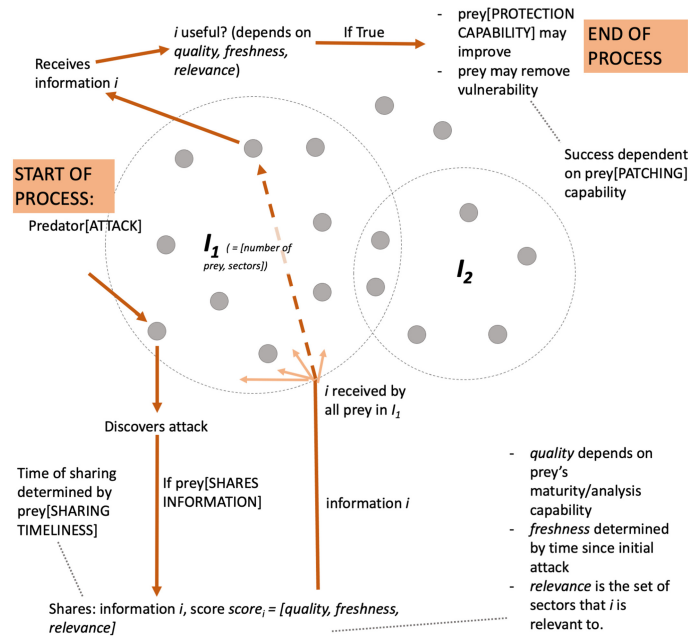


Fig. 3. Model of the prey-community information-sharing process.

We model the following actions by prey in receipt of the information:

- Change from patching according to the “normal” patching probability to the “prompted” probability.
- Improve their PROTECTION CAPABILITY (generally representative of protective controls such as firewalls and employee awareness) with a higher (prompted) probability.

For the simulations presented in this article, we represent a simple example of a highly effective information-sharing process. In particular, we present the case in which there is only one information-sharing community, in which prey either participate or do not. We assume that all prey that share information do so with high

timeliness (immediately after compromise), high quality, and relevance. We therefore assume that information shared is useful to all prey who receive it.

#### 4.5 Functions

Functions describe the actions that predators (D) and prey (Y) can take in each state (Clean (O), Infected (I), Compromised (C), and Recovering (R)). Each function is called with an assigned probability, which may depend on parameters of the predator and prey. Probabilities of the form  $p_{XYN}$  describe the probability that a function is called. The subscripts in the notation describe whether  $X$  is a predator or prey function (D/Y), the state  $Y$  that it is called from (O/I/C/R), and an identifying number  $N$ .

Probabilities of the form  $p_{XYN-P}$  describe the probability that a function is called under “prompted” conditions. Certain actions, such as patching or disconnecting, might be taken at any time, but are more likely to be taken under certain conditions (e.g., immediately following discovery of an attack). To represent this, such functions have separate probabilities under “normal” and “prompted” conditions.

Functions with both “normal” and “prompted” probabilities are:

- CONNECT: prompted in the CLEAN state
- REMOVE VULNERABILITY and IMPROVE PROTECTION CAPABILITY: prompted:
  - if REMOVE RANSOMWARE BINARY is called (i.e., the ransomware is detected) in the INFECTED state
  - after successfully cleaning a ransomware compromise
  - when in receipt of threat-intelligence information
- DISCONNECT: prompted in the COMPROMISED state

Tables 6–8 show the complete list of functions available to the prey, predator and world agents from each state, the probability of each function being called, and the justifications for including these functions and probabilities in the model. Where these function probabilities are dependent on one or more predator or prey parameter values, the assignment of probability for each possible combination of parameter values is shown.

The probabilities refer to the probability of a function being called at each step of the model. We chose to model a “step” of the model as a day. Based on the time periods ransomware attacks usually last for, we posit that days are a sufficiently granular timespan for modelling and abstraction of the actions taken by predators and prey during a ransomware attack. For example, in a survey of IT and security professionals, 66% of companies estimated it would take five or more days to fully recover from a ransomware attack if they did not pay the ransom [3]; another survey stated that in 2021 one month was the average time taken to recover from an attack [10]; while Yuryna-Connolly et al. found that across 55 ransomware cases, interruptions as a result of ransomware attacks were likely to last days (rather than hours), and dependent on the severity of the impact, it could take up from up to one week to more than two weeks to regain business continuity, and in more severe cases it could take months for the organisation to fully recover [77].

**4.5.1 Justifications for Function Probabilities.** We present support for our assignment of probabilities to functions. As we discuss in Section 7, there is a lack of data to support the probabilities that organisations take various defensive actions, and we have therefore had to make various assumptions based on limited data.

**Prey functions: Protection:** We assume that organisations with higher PROTECTION CAPABILITY are more likely to succeed in preventing delivery of ransomware. We assign the probability of preventing delivery to be  $\text{PREY}[\text{PROTECTION CAPABILITY}]$ : {“HIGH”: 0.9, “MEDIUM”: 0.5, “LOW”: 0.1}. In the absence of evidence to support more specific treatment, we use these as a standard set of values for most of the function probabilities determined by H/M/L prey capabilities (protection, detection, and response).

**Detection:** We assume that organisations with “high” DETECTION CAPABILITY will detect types of ransomware with “low” or “medium” HARDNESS OF DETECTION with higher probability. We assume that organisations with

Table 6. Prey Functions

Function	State	Description	Probabilities	R
PREVENT DELIVERY	0	prey prevents delivery of the ransomware through protective controls	$p_{OY1}$ : PREY[PROTECTION CAPABILITY]: {"HIGH": 0.9, "MEDIUM": 0.5, "LOW": 0.1}	R3
REMOVE RANSOMWARE BINARY	I	prey removes ransomware before execution	$p_{IY1}$ : PREY[DETECTION CAPABILITY][PREDATOR[HARDNESS OF DETECTION]]: {"high": {"high": 0.5, "medium": 0.9, "low": 1.0}, "medium": {"high": 0.1, "medium": 0.5, "low": 0.9}, "low": {"high": 0, "medium": 0.1, "low": 0.5}}	R6
CLEAN RANSOMWARE	C	prey cleans its systems of the executed ransomware	$p_{CY1}$ : PREY[RESPONSE CAPABILITY][PREDATOR[HARDNESS OF CLEANING]]: {"high": {"high": 0.5, "medium": 0.9, "low": 1.0}, "medium": {"high": 1, "medium": 0.5, "low": 0.9}, "low": {"high": 0, "medium": 0.1, "low": 0.5}}	R11
RESTORE BACKUPS	C, R	prey restores from backups, thus fixing impacts and removing ransomware	$p_{CY2}$ : if not PREY[BACKUPS] = "none": PREY[RESPONSE CAPABILITY]: {"high": 0.9, "medium": 0.5, "low": 0.1}, else: 0	R11d
DISCARD ASSETS	C, R	prey discards impacted assets, fixing impacts	$p_{CY3}$ : 0.1	R11e
REMOVE VULNERABILITY	O,I,C,R	prey removes vulnerability to the ransomware (patch)	$p_{OY2-P}$ : PREY[RESPONSE CAPABILITY]: {"high": 0.9, "medium": 0.5, "low": 0.1, "none": 0}; $p_{OY2}$ : PREY[PATCHING]: {"high": 1, "medium": 0.1, "low": 0.01, "none": 0}	R4c, R11f
IMPROVE PROTECTION CAPABILITY	O,I,C,R	prey improves their protection capability ("low" $\rightarrow$ "medium," "medium" $\rightarrow$ "high")	$p_{OY3-P}$ : 0.5; $p_{OY3}$ : 0	R11f
CONNECT	O,I,C,R	prey connects to the threat vector through which the ransomware attacks (e.g., Internet)	$p_{OY4-P}$ : 1; $p_{OY4}$ : 0	R11c
DISCONNECT	O,I,C,R	prey disconnects from the threat vector	$p_{OY5-P}$ : PREY[RESPONSE CAPABILITY]: {"high": 0.9, "medium": 0.5, "low": 0.1}; $p_{OY5}$ : 0	R11c
PAY RANSOM	C,R	prey pays ransom in an attempt to fix impacts	$p_{CY4}$ : if predator not in PREY[UNSUCCESSFUL RANSOM PAYMENTS]: PREDATOR[PAYMENT PRESSURE][PREY[PAYS RANSOMS]]: {True: {"high": 0.9, "medium": 0.5, "low": 0}, False: {"high": 0.45, "medium": 0.25, "low": 0}}, else 0	R11a, R14a
OTHERWISE FIX	C,R	prey fixes impacts another way (e.g., breaking weak encryption using available tools)	$p_{CY5}$ : PREY[RESPONSE CAPABILITY]: {"high": 0.9, "medium": 0.5, "low": 0.1}	R12
SHARE INFORMATION	C	prey shares information to the WORLD agent following an attack	$p_{CY6}$ : 1 if PREY[SHARES INFORMATION], else 0	R11b, R16

**R:** Reference to supporting modelling requirement.

Table 7. Predator Functions

Function	State	Description	Probabilities	R
PREDATOR ATTACK	O	predator attacks prey	for up to $\text{PREDATOR}[\text{ATTACK BANDWIDTH}]$ prey per time unit: $p_{OD1} = 1$ if prey matches predator[proximity factors]	<b>R1</b>
EXECUTE	I	ransomware executes on system	$p_{ID1} = 1$ if number of time units in INFECTED state $\geq \text{PREDATOR}[\text{TIME TO EXECUTE}]$	<b>R5</b>
IMPACT	I	ransomware causes its intended impacts to prey after execution	$p_{ID2} = 1$	<b>R7</b>
DESTROY BACKUPS	I	ransomware destroys prey's backups after execution	$p_{ID3} = 1$ if $\text{PREDATOR}[\text{DESTROYS BACKUPS}]$ ; else 0	<b>R8</b>
PROPAGATE ATTACK	C	ransomware propagates attack from host prey to other prey	$p_{CD1} = 1$ if $\text{PREDATOR}[\text{PROPAGATES}]$ (predator propagates attack to selected number of prey based on $\text{PREDATOR}[\text{PROPAGATION BANDWIDTH}]$ )	<b>R9</b>
IMPACT	C	ransomware left on system impacts prey	$p_{CD2} = 1$ if $\text{PREDATOR}[\text{REIMPACTS}]$ ; else 0	<b>R10</b>
BECOME INACTIVE	O,I,C,R	predator becomes inactive as a result of not receiving ransom payments	$p_{OD2} = 1$ if number of steps since predator received last ransom payment $\geq \text{PREDATOR}[\text{INACTIVE THRESHOLD}]$ ; else 0	<b>R15</b>

**R:** Reference to supporting modelling requirement.

Table 8. World Functions

Function	State	Description	Probabilities	R
CREATE PATCH	O,I,C,R	world creates a patch against a ransomware	$p_{W1} = 0.1$	<b>R4b</b>
CREATE IMPACT FIXING TOOL	O,I,C,R	world creates an impact-fixing tool for a ransomware	$p_{W2} = 0.2 \times \text{PREY}[\text{HARDNESS OF IMPACT FIXING}]$ : {"high": 0.1, "medium": 0.5, "low": 0.9}	<b>R12</b>

**R:** Reference to supporting modelling requirement.

“low” DETECTION CAPABILITY have a low chance of detecting ransomware before execution and will not detect ransomware with “high” detection hardness.

**Response functions:** We assume that organisations with higher levels of RESPONSE CAPABILITY are more likely to take the actions recommended by various guidance sources (R13):

- Organisations with “high” RESPONSE CAPABILITY are more likely (than those with “medium” or “low” response capability) to take the following actions in response to compromise: successfully clean ransomware; restore from backups (if they have them); otherwise fix impacts; disconnect from the threat vector; remove vulnerability.
- Organisations with “high” RESPONSE CAPABILITY are unlikely to pay the ransom, since most guidance recommends against this, and this is therefore assigned a lower probability for organisations with higher RESPONSE CAPABILITY. We assume that organisations with “low” RESPONSE CAPABILITY take these recommended actions with a lower probability and are relatively more likely to pay the ransom earlier. We assume that organisations with all levels of RESPONSE CAPABILITY are more likely to pay the ransom if the attacker applies payment pressure.

In the absence of evidence to support more specific treatment, the probabilities used are the same for these functions:  $\text{PREY}[\text{RESPONSE CAPABILITY}]: \{ \text{“HIGH”}: 0.9, \text{“MEDIUM”}: 0.5, \text{“LOW”}: 0.1 \}$  (and the converse for ransom payment:  $\{ \text{“HIGH”}: 0.1, \text{“MEDIUM”}: 0.5, \text{“LOW”}: 0.9 \}$ ).

**Vulnerability removal:** In the “prompted” cases, vulnerability-remediation probabilities are handled in line with the treatment of response functions described above. In the unprompted case (i.e., patching following the organisation’s normal patch cycle), we model daily patching for organisations with “high” PATCHING CAPABILITY (since an automatic patching tool such as Windows Update will check for updates at least daily) and quarterly patching for organisations with “low” PATCHING CAPABILITY.

**Connecting and disconnecting:** For disconnecting in the “prompted” case, the probability is handled in line with the treatment of response functions described above. The likelihood of disconnecting in an unprompted case is very low—for this simulation, we set the probability to 0.

The probability of connecting to the Internet in the prompted case (after becoming CLEAN) is very high—we set the probability to 1. In an unprompted case, the probability of connecting is very low—we set the probability to 0.

**Discarding:** The probability that a prey discards their data is lower; we assume that this action is likely to be taken as a last resort. Furthermore, in the absence of evidence supporting assignment of probability according to response capability (since the action is recommended neither for nor against by guidance), a single value is used.

**World functions: Creating patches:** We use 0.1 as the probability that a patch is created at each step. This reflects statistics from a Mandiant study of vulnerabilities, which showed the average time between disclosure and patch availability to be approximately nine days [44].

**Creating impact-fixing tool:** This probability is determined based on the predator’s HARDNESS OF IMPACT-FIXING value. In the absence of other evidence, we assign the same probability as for patch creation for the creation of tools to fix ransomware with “medium” hardness and vary the probability in the case of ransomware with “low” and “high” hardness, relative to the standard H/M/L treatment scale described (i.e.,  $0.2 * \{0.1, 0.5, 0.9\}$ ).

## 4.6 Simulations

Figure 4 shows a simplified timeline view of how the prey moves through a series of states as various predator and prey actions are taken. Our simulations are implemented in timesteps, where at each step the following actions are taken by prey and predators in random order:

- Active predators check for susceptible prey and attack a certain number of these susceptible prey, dependent on  $\text{PREDATOR}[\text{ATTACK BANDWIDTH}]$ . For simplicity, in the simulations presented in this article, predators only attack prey that are in the Clean state.

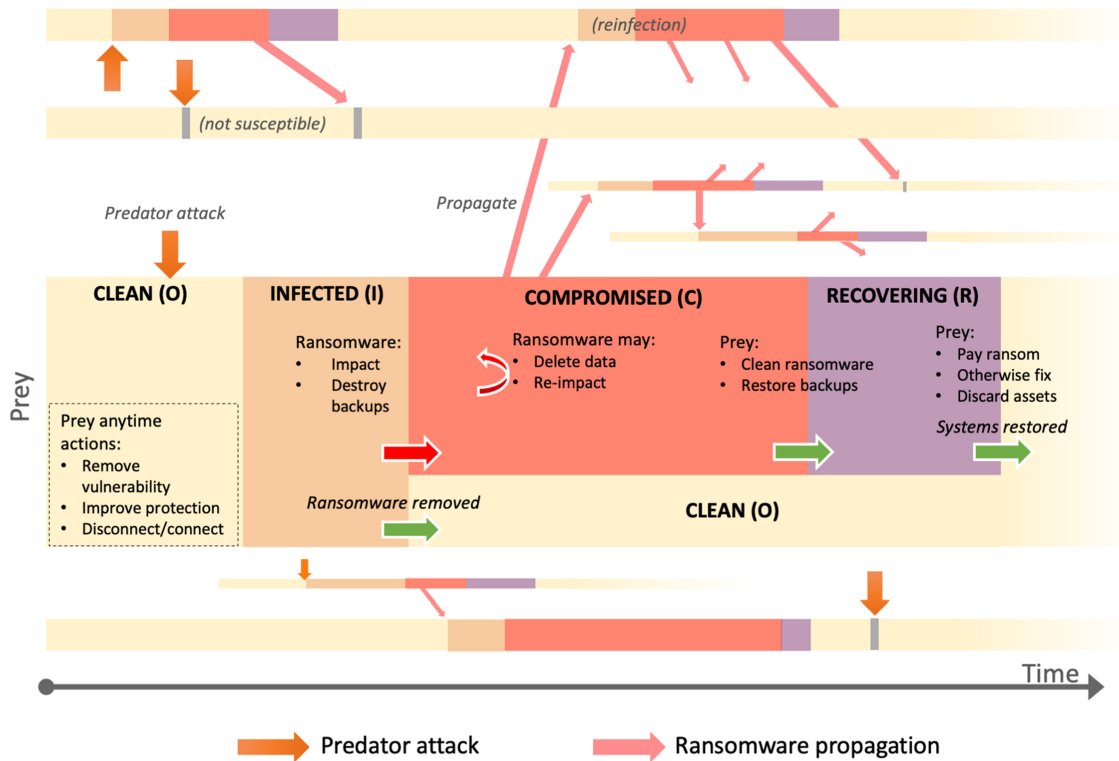


Fig. 4. Timeline view of predator and prey states and actions in the general ransomware model.

- Prey functions are called, determined by the current state of the prey with respect to the predator, which may update the prey's state with respect to that predator. For example, as shown in Figure 2(a), if the prey has been INFECTED, then prey functions including REMOVE RANSOMWARE BINARY() may be called with some probability, which could transition the prey to the CLEAN state.
- Predator functions are called in the prey according the current state of the prey with respect to the predator, which may update the prey's state with respect to that predator. For example, as shown in Figure 2(a), if the prey has been INFECTED by predator X, then predator functions including EXECUTE() may be called, which could transition the prey to a COMPROMISED state with respect to predator X.
- A number of prey functions may be called from any state with certain probabilities (the "Anytime functions" in Figure 2(a), which may update the state of the prey. If these functions relate to IMPACTS (i.e., the functions that are called if PREY[IMPACTS] is non-empty in Figure 2(a)), then they are called with respect to the predator that has created that impact (e.g., Predator Y who has impacted the prey would be paid a ransom if the prey function PREY[PAY RANSOM()] were called). It is important to note that this approach considers the PREY[IMPACTS] changes made by each predator to be distinct—i.e., if one predator impacted the prey, then another predator could also impact the prey. It represents the case where different predators cause impacts on prey that can be fixed through distinct actions, but in reality the interplay between simultaneous impacts by multiple different predators may increase the complexity of fixing them (e.g., if the same pieces of data became encrypted multiple times).

In states where there are multiple actions available to the prey, the prey calls response functions per step according to these assumptions:

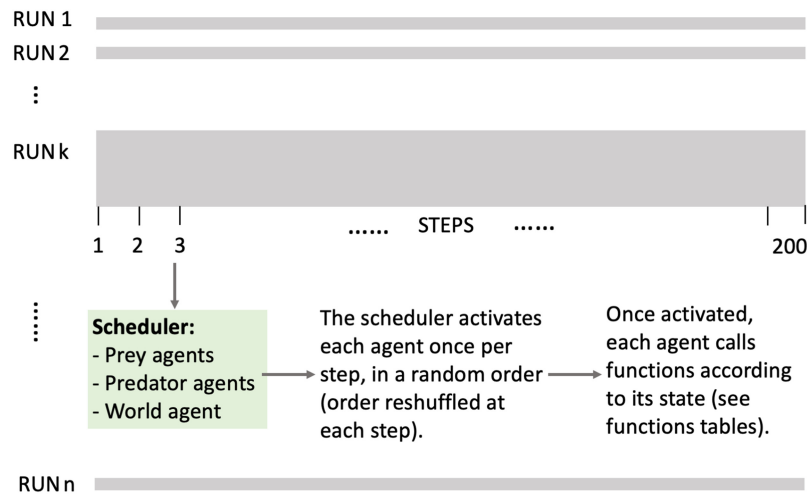


Fig. 5. High-level diagram of the simulations process.

- Maximum one response action can be taken by prey in each iteration (e.g., pay ransom or clean ransomware).
- At each step, whether the prey or the predator acts first is randomised, and their actions are decided based on the prey's state. If the actions of the first party to act move the prey to a new state, then the other party does not act in this step.
- If a prey pays a ransom to a predator, and the predator does not respond to it (by fixing the impacts), then that prey will not pay that predator again.

All available functions are added to a temporary possible function calls list with some probability (their assigned function call probability). A random function is then chosen from the temporary function calls list, to be performed in that iteration.

#### 4.7 Implementation

The model was implemented in Python using the Mesa agent-based modelling framework. Figure 5 presents a high-level description of how the simulation was conducted.

### 5 WANNACRY CASE STUDY: ASSIGNMENT OF PREDATOR PARAMETER VALUES AND PREY CLASSES

#### 5.1 Overview of the WannaCry Ransomware Outbreak

The WannaCry ransomware outbreak in May 2017 impacted an estimated 300,000 machines in organisations in over 150 countries worldwide. A wide range of sectors including Telecommunications, Healthcare, Energy, and Transport were impacted, with estimated losses of \$4 billion [1].

WannaCry had two key elements:

- **Ransomware binary.** Encrypted files and demanded a ransom.
- **Worm functionality.** Automatic spreading from infected machines to others as a worm.

*Vulnerability and execution.* WannaCry targeted machines using their IP address and exploited a vulnerability in the SMB communication protocol used by Windows machines to communicate with file systems (widely used for file-sharing between organisations). It leveraged the EternalBlue software to exploit vulnerabilities in the

Table 9. Predator Agent Parameters: Constant Parameters (WannaCry)

Parameter	Value
Bandwidth	30
Responds to payment	False
Attracted to	{sector: [“regulated,” “unregulated”], revenue: [“high,” “medium”]}
Attack surface required	{tech vulnerabilities: [“eternalblue”], firewall: “poor”}
Time to execute	1
Propagates	True
Propagation bandwidth	50
Re-impacts	False
Hardness of impact fixing	Medium
Hardness of detection	Medium
Hardness of cleaning	Medium
Destroys backups	False

implementation of the SMB protocol on external-facing server message ports. By exploiting this vulnerability, it implanted the Doublepulsar backdoor, Which was then used to execute WannaCry on the compromised system [49].

A patch for the EternalBlue vulnerability was available at the time of the outbreak, but many companies had not applied it. The security-patch timeline was as follows:

- First WannaCry samples were seen in VirusTotal in February 2017.
- Microsoft release SMB updates for supported OS’s (not Windows XP or 2003) in March 2017 (MS17-010 security patch)
- SMB updates for XP and 2003 were released the day after the outbreak began.
- WannaCry advisory was published March 14, 2017; outbreak date was May 12, 2017 (59 days later)

When WannaCry executed, it encrypted the files of the victim systems.

*Propagation.* Once it had compromised a machine on a network, the ransomware was capable of propagating internally to other machines on the network and externally over the Internet [13]. There was no requirement for user interaction to enable virus propagation.

- **Local network attack.** The IP address of the infected machine was checked and the ransomware probed for SMB ports and attempted exploits on each IP address in the same subnet. The local IP subnet scan was multithreaded, but the ransomware limited it to 10 IP addresses per scan to avoid detection from the CPU overhead.
- **Internet attack.** The ransomware generated random IP addresses on the Internet to perform the same action as above. 128 threads were created for this external scan, meaning that in organisations with infected machines, each of its machines could have been trying to infect up to 128 routable/24 subnets. It is likely that the “bridgehead” into a network would in most cases have been a server exposing SMB services to the Internet, since most organisations do not assign routable addresses to their workstations [70].

## 5.2 Predator Agent Parameters

Table 9 shows the predator-agent parameters assigned to represent the WannaCry ransomware attack.

For practicality of running the simulations, we scaled down the number of prey to 10,000 (whereas approximately 300,000 victims were affected in the real attack, as above). Other factors required scaling to match this: the number of predators, attack bandwidth, and propagation bandwidth. While it is challenging to be exactly

accurate in the face of limited data, we sought to identify representative orders of magnitude. Since each infected machine was able to propagate to 128 others simultaneously, as above, and we assume each thread attacked at a minimum once every 1–2 hours, we assume each machine could propagate the attack to at least 1,500 others per day (scaled down to propagation bandwidth of 50 per step, according to our scale factor).

There is little evidence on the number of attackers or their attack bandwidth; we therefore assumed approximately 1,000 for each, which was then scaled as above. Note that propagation bandwidth and the number of predators were two factors we experimented with varying the value of; the below is only the baseline value assigned.

### 5.3 Prey Classes

We define four classes of prey (organisations) to be used in the simulations. While there are many possible permutations of the prey parameters' values that could be used, in these simulations, we sought to represent realistic classes of organisation and to compare how classes of prey with different levels of cybersecurity capability fare in the face of a propagating ransomware attack, including when specific community defensive actions are taken.

To enable this comparison, we chose to model classes with a high level of capability (protection, patching, detection, and response), a medium level and a low level. In the absence of evidence suggesting that it is common for organisations to vary across different types of capability (e.g., to have high levels of protective capability and low levels of response capability), we considered it most likely that organisations would be similarly capable across the capabilities (particularly since most widely used cybersecurity standards cover all of these types of capability, so it is likely that those organisations following cybersecurity standards would achieve a higher level across them). Therefore, each class of organisation was assigned either a high, medium, or low level across these capabilities.

- Class A represents the “highest” maturity class. It is modelled as organisations from a regulated sector with high revenue. They have generally high levels of cybersecurity maturity: high levels of protection, detection, and response capability. Organisations in this class keep secure backups and pay ransoms with low probability (since, as discussed, ransom payment is unrecommended by guidance and, therefore, we model organisations with higher levels of cybersecurity maturity as less likely to pay ransoms).
- Class B represents the “medium” maturity class. It is modelled as organisations from a regulated sector with medium revenue. They have a medium level of protection, detection, and response capability. They keep data or system backups, although these are not fully secure, and pay ransoms with medium probability.
- Class C represents the “low” maturity class. It is modelled as organisations from an unregulated sector with medium revenue. They have generally poor cybersecurity maturity: low levels of protection, detection, and response capability and do not keep backups. They pay ransoms with high probability.
- Class D is modelled as organisations who are unable to patch their systems against the ransomware (noting that they may still improve their general protection capability). This is representative of organisations who use technology that is no longer supported or cannot be upgraded for functionality reasons (such as the need to retain older versions of systems for their specific functionalities and compatibilities), for example. It is modelled as identical to Class C, but with the inability to patch.

Table 10 and 11 show the parameter values assigned to represent these four classes of organisation. The class distribution used in the simulations was:

- Class A: 3/10 of the prey
- Class B: 3/10 of the prey
- Class C: 3/10 of the prey
- Class D: 1/10 of the prey

Table 10. Case Studies: Prey Agent Parameters (Constant)

Parameter	Class A	Class B	Class C	Class D
Sector	regulated	regulated	unregulated	unregulated
Revenue	high	medium	medium	medium
Tech vulnerabilities	[eternalblue]	[eternalblue]	[eternalblue]	[eternalblue]
Patching	high	medium	low	none
Protection capability	high	medium	low	low
Detection capability	high	medium	low	low
Response capability	high	medium	low	low
Pays ransoms	low	medium	high	high
Shares information	False	False	False	False
Propagation controls	False	False	False	False

Table 11. Case Studies: Prey Agent Parameters (Variable)

Parameter	Class A	Class B	Class C	Class D
Connected	True	True	True	True
Impacts	[]	[]	[]	[]
Backups	secure	insecure	none	none

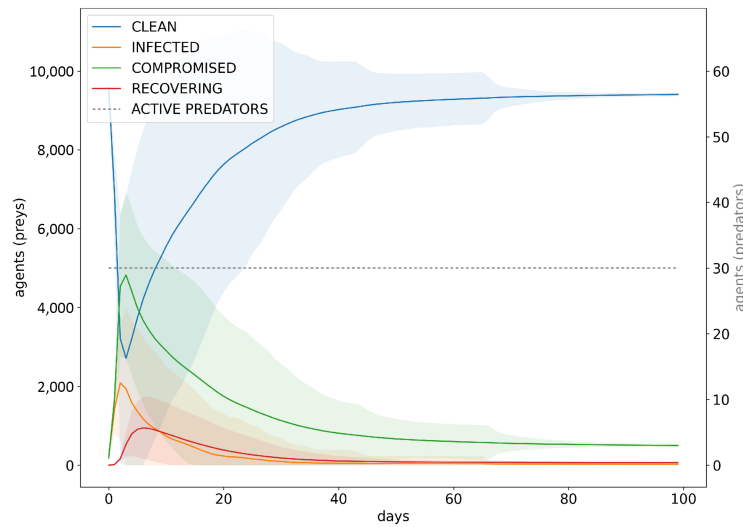


Fig. 6. Baseline simulation.

## 6 WANNACRY CASE STUDY: RESULTS

We ran the simulations over 100 steps (days). We used Monte Carlo simulation, running 300 simulations per scenario.

### 6.1 Baseline Simulation

Figure 6 shows the results of the baseline simulation, run according to the parameters described in the previous section, with 30 predators. The plots show the mean (across simulations) number of prey in each state (Clean,

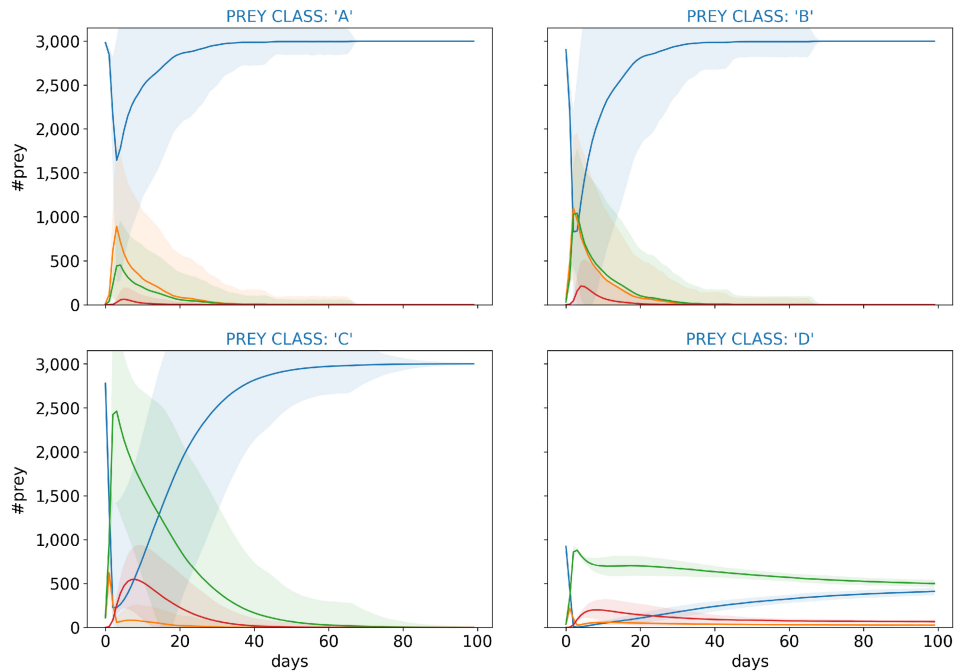


Fig. 7. Healthiness conditions: Behaviour of the individual classes in the simulation.

Infected, Compromised, and Recovering) and the number of active predators. The shaded areas show two standard deviations from the mean.

## 6.2 Model Healthiness

We verified the healthiness of our model and implementation by testing a set of healthiness conditions relating to the behaviour of the individual classes:

- For organisations in Class A, it should be true that a smaller proportion (than in the other classes) become compromised, since these organisations are less likely to be susceptible to the ransomware (have higher protection capability and patching practice). It should also be true that those organisations that are compromised recover more quickly, on average, relative to the other classes, since organisations in this class have higher levels of detection and response capability.
- For organisations in Class B, the proportion of prey compromised should be higher than for Class A, but low compared to Classes C and D. The recovery rate should also be faster than for Classes C and D.
- For organisations in Class C, it should be the case that a very high proportion of organisations become compromised simultaneously, and the recovery rate is relatively slow.
- For organisations in Class D (the same as Class C but with inability to patch), again, it should be the case that a very high proportion of organisations become compromised simultaneously, and furthermore that the number of prey compromised may reduce more slowly than in other classes (since prey cannot patch, but may take other actions such as improving their protection capability over time).

Figure 7 shows that these healthiness conditions were met (this shows the breakdown of the baseline simulation plot into the individual classes).

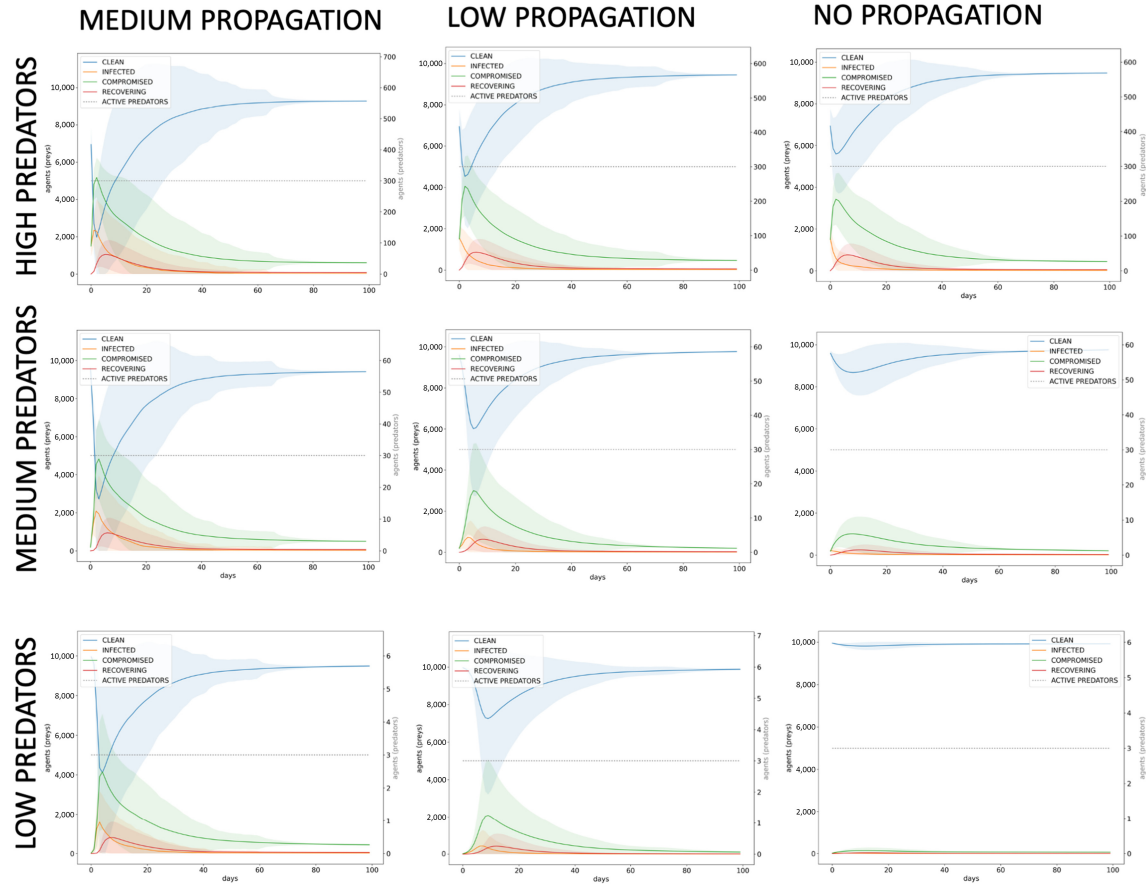


Fig. 8. Baseline. Number of predators H/M/L; propagation rate H/L and none (i.e., all propagation prevented).

### 6.3 Measuring Systemic Risk

Based on the understanding of systemic cyber-risk introduced in Section 1 as being the possibility that a large number of organisations will be negatively impacted by a single event, we consider two metrics:

- Maximum number of prey simultaneously compromised (i.e., at the same step) by a single weapon (in this case study, WannaCry). This is relevant, since it provides an indication of the largest event size observed as a result of the single trigger.
- Rate of recovery from the maximum. This provides an indication of the length of time for which a high level of compromise persists across the community of organisations.

### 6.4 Effectiveness of Propagation Controls, Not Paying the Ransom, and Information Sharing

We explored the effect of a high (300), medium (30), and low (3) number of predators, and a medium (50) and low (5) propagation rate, on the output plots for propagation controls, not paying the ransom, information sharing (and various combinations of these). We explored the effect of varying the number of predators and the propagation rate based on a hypothesis (developed based on exploratory experimentation) that these two factors impact on the effectiveness of the controls under investigation.

**6.4.1 Varying the Number of Predators and Propagation Rate; Use of Propagation Controls.** Figure 8 shows the effect of these variations to number of predators and propagation rate on the baseline simulation.

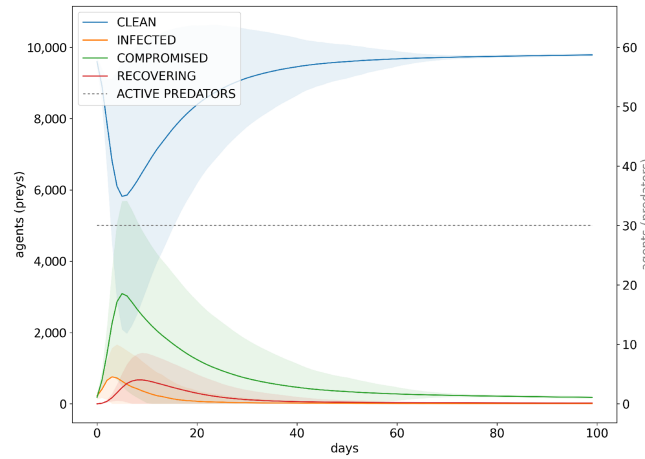


Fig. 9. Classes C and D have propagation controls (propagation: medium; number of predators: medium).

Preventing some or all classes from propagating the ransomware (representing the case where certain classes of prey are able to implement controls that prevent propagation) is the control that had the most significant effect consistently across settings. The third column of Figure 8 shows the results of propagation being prevented completely (which represents the case of either a non-propagating ransomware or a propagating ransomware outbreak in which all prey have completely effective propagation controls), while Figure 9 shows the results of Classes C and D implementing propagation controls (with propagation rate: medium; number of predators: medium). In all cases of high/low predator and propagation rate, preventing propagation significantly reduced the maximum number of prey compromised.

**6.4.2 Not Paying the Ransom.** Figure 10 shows the effect of prey not paying the ransom, where the predator becomes inactive after 10 steps of not being paid any ransom. It can be observed (comparing these plots to the baseline in Figure 8) that using this control in these settings does not have a significant effect on the maximum number of prey compromised.

The predators are set to become inactive after 10 steps of not receiving ransom payment. As such, the plots show that the number of predators drops only after 10 steps, by which time the maximum number of compromised prey has already occurred and the number compromised is already decreasing. This suggests that not paying the ransom will only reduce the maximum number of prey compromised in cases where this maximum is reached after predators start to become inactive (e.g., in cases where predators become inactive sooner after not receiving ransom payments). These observations are to be expected for a single instance of ransomware; it may be that over longer periods of time with multiple ransomware variants and mutations, not paying the ransom makes a more significant difference, and we consider this further in Section 7.

However, not paying the ransom does affect the recovery rate of prey. In particular, the number of compromised prey eventually returns to zero when the prey do not pay the ransom and the propagation rate is low or none. This is to be expected, since predators have ceased attacking, and the propagation is sufficiently low that the outbreak stops. This also suggests the criticality of propagation controls to bolster the effectiveness of other types of control (policies against ransom payment in this case).

**6.4.3 Information Sharing.** Figure 11 shows that information sharing made some observable difference in these settings to the maximum number of prey compromised and the recovery rate of the population of prey, particularly when the number of predators and the propagation rate were low. We hypothesised that the reason for observing little effect when the number of predators and propagation rate were higher was that, similarly to

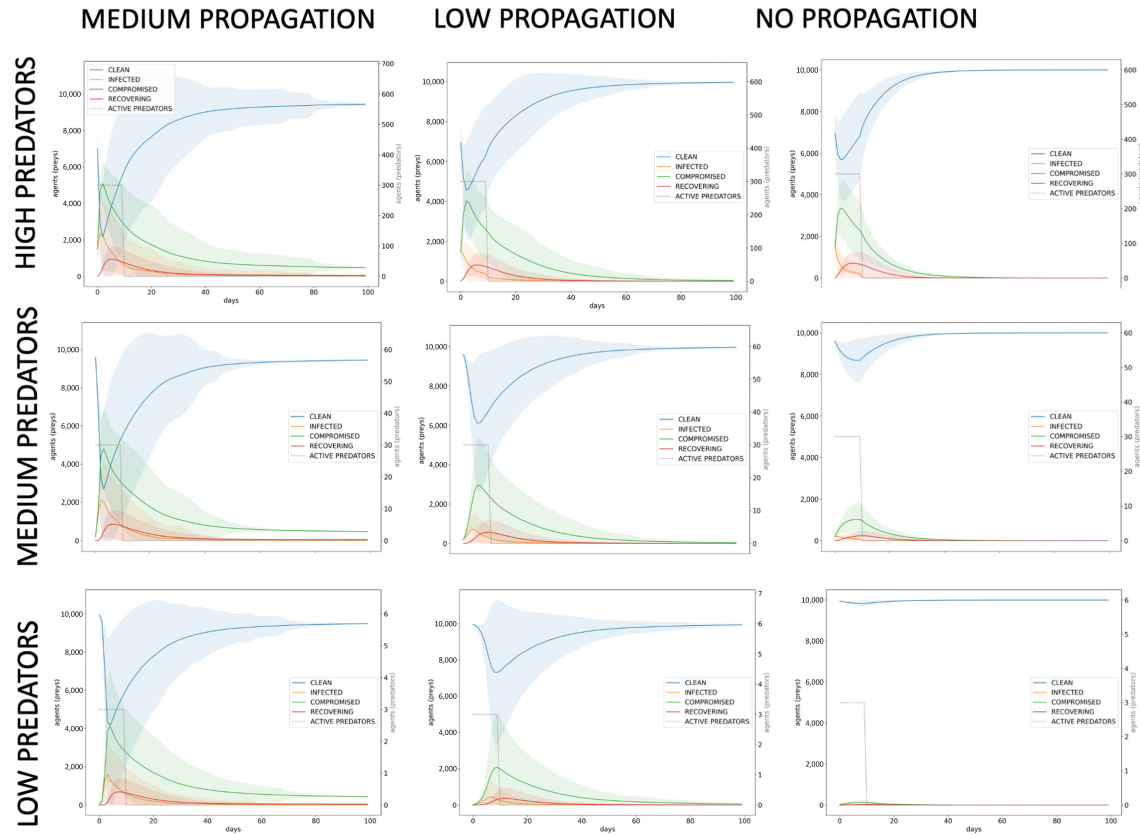


Fig. 10. All prey do not pay the ransom. Predators inactive after 10 steps without payment. Number of predators H/M/L; propagation rate H/L and none.

in the “not paying the ransom” case, the maximum compromised was being reached too quickly for information-sharing to take effect and was already decreasing by the time information-sharing took effect. We hypothesised that there is a balance between the quality of information-sharing practices and the speed at which prey are compromised, which needs to be met if information-sharing is to make a significant difference to the number of prey compromised.

To test this hypothesis, we simulated a “highly effective” version of an information-sharing community (in which the information-sharing threshold was lowered (from [20, 50] to [5, 10]), and the probability of the “world” creating a patch at each step was increased (from 0.1 to 0.5). We explored the case of low propagation rates and number of predators, which causes the peak number of prey compromised to be delayed. Figure 12 shows the results: With these settings, information sharing and the higher likelihood of patch availability (enabling those prey receiving information to patch) cause the maximum compromised to be lower and the decrease in the number compromised after this peak to be significantly faster, supporting the hypothesis.

## 7 DISCUSSION

These simulations enable us to reason about the individual and combined impacts of the three defensive approaches under study on mitigating systemic risk, and the factors that may affect the efficacy of these approaches.

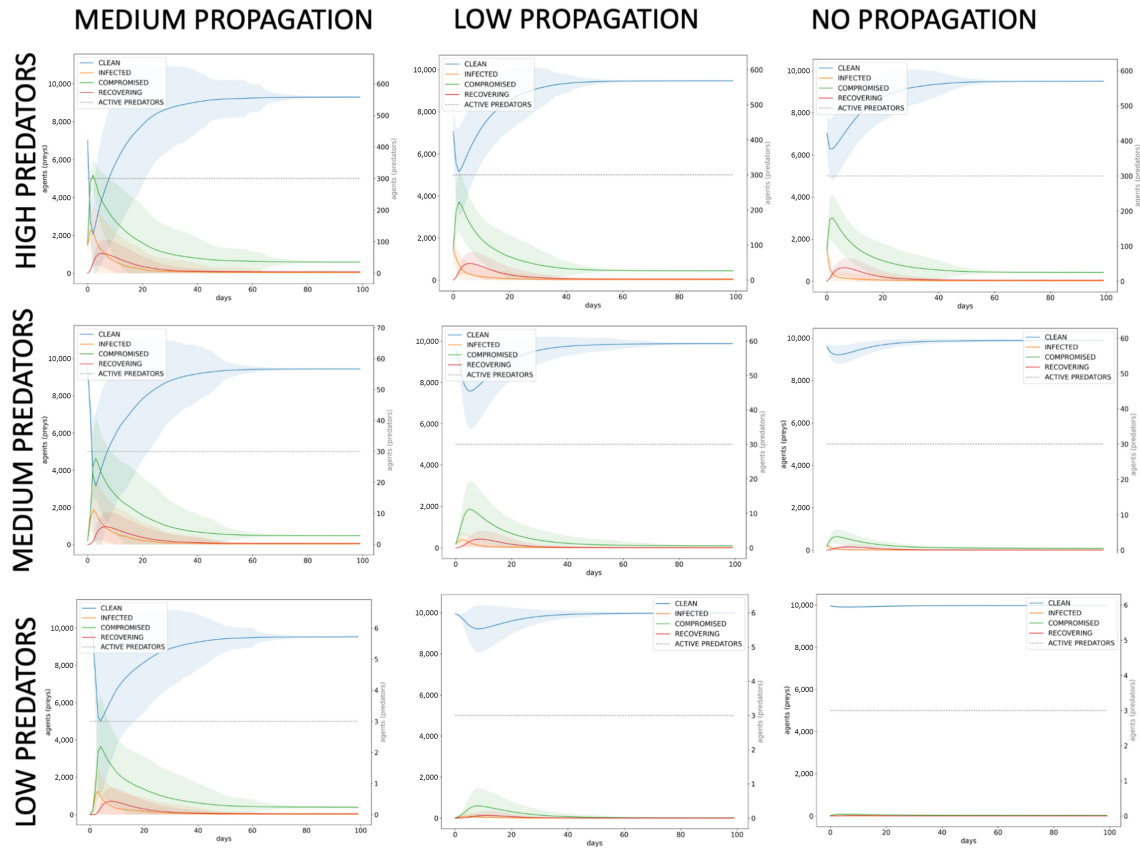


Fig. 11. All prey share information; information-sharing thresholds 20 (“consumers”), 50 (“big news”). Number of predators H/M/L; propagation rate H/L and none.

### 7.1 Propagation Controls

The results suggest the criticality of controls that can prevent onward propagation of ransomware, to mitigate systemic risk from propagating ransoms. As we showed, controlling propagation consistently had a significant impact on reducing the number of compromised prey. It also made the other types of control under study (information sharing and not paying the ransom) more impactful than they were otherwise. Controlling propagation positively impacts the entire ecosystem of susceptible organisations, yet propagation can only be controlled through the actions taken by individual organisations; i.e., there may be a need for organisations to take on more responsibility to implement propagation controls to reduce the systemic risk to the collective.

In practice, controls that prevent onward propagation would likely take the form of outgoing firewall rules (including automated through intrusion-prevention systems); disconnection from relevant communications vectors (again, potentially automated); and potentially automated controls that directly target code with propagation functionalities, detecting it, and preventing it from executing. The development of controls to be deployed in individual organisations, which can act quickly to prevent propagation, is critical.

There may also be a community element to the prevention of propagation; for example, the community may focus not only on distribution of patches against a particular threat at the time of an outbreak, but also on distribution of, e.g., firewall rules to prevent propagation of the threat. As we have seen, in many of the simulations organisations that cannot patch—Class D—become constantly reinfected, and establishing methods such as these

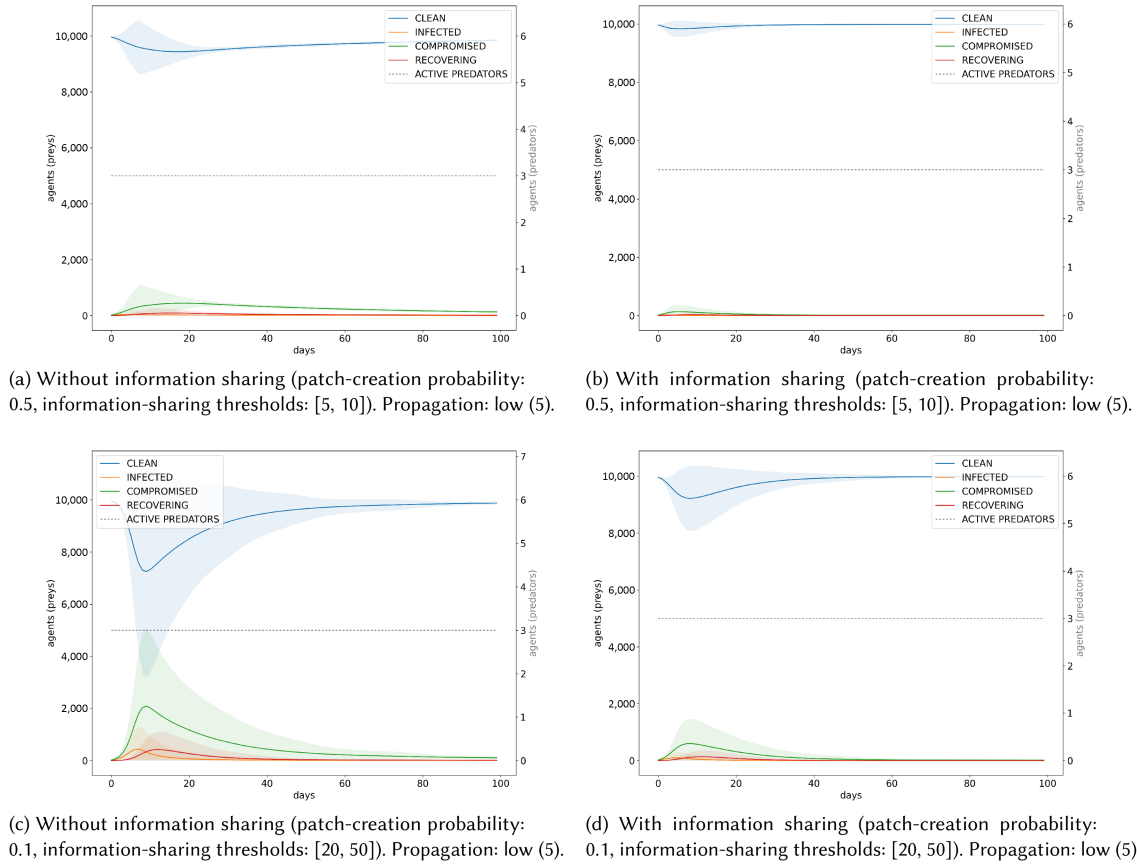


Fig. 12. Comparison between a “highly effective” version of information sharing (lower information-sharing thresholds and higher patch-creation probability) and a less effective version. Number of predators: low (3).

that can prevent propagation of a threat even between organisations that cannot patch against is important to prevent the systemic risk from lingering and continuously propagating between such organisations.

## 7.2 Ransom Payment

Whether or not companies should pay ransoms is a complex issue and a subject of recent scrutiny. As we noted earlier, ransom payment is discouraged by most reputable guidance sources and law enforcement [5, 6], yet many victim organisations are still paying ransoms. It has been reported that the average ransom paid by mid-sized organisations in 2020 was \$170, 404 dollars [9] (in some cases, very large sums, as in the recent example of the ransomware attack on Colonial Pipeline, in which the victims paid a ransom of around \$5 million [73]). Furthermore, there is an ongoing discussion about whether countries should legislate against ransom payments [56], and some insurers have removed ransomware coverage from their offerings [42].

A prey policy against ransom payments could have an impact on the activity and tactics of the predator population. It is reasonable to assume (and has been observed in reality—see Section 3) that a predator that is not receiving ransom payments might simply become inactive, ceasing to launch ransomware attacks. They might also change their tactics to using different types of ransomware, putting different pressures on the victims (e.g., by threatening to leak data), or targeting a different victim population.

In our modelling, we have represented the former case (predator becomes inactive), with results suggesting that, in the case of a single attack (i.e., by one set of attackers, using a single ransomware variant over a limited time period), a prey policy against ransom payments could improve the ability of the prey population as a whole to recover to an uncompromised state. In light of the discussion above, there would be value in expanding this work to explore the impact of ransom payment on predators and therefore systemic risk over a longer period of time, considering multiple strains and mutations of ransomware, and a broader range of predator tactics in response to no-payment. Data collection on this topic would also be valuable to understand the real impacts of no-payment policies on predators' actions.

### 7.3 Information Sharing

We found that a number of factors impact the effectiveness of information-sharing as a control against systemic risk: the speed with which threat information becomes available to organisations; the speed of the security community in developing a patch against the threat and making it available across organisations; and the speed with which organisations in receipt of the information patch against the threat. Even in cases where these processes are highly effective, however, they may have little impact against a ransomware that is propagating very quickly.

These factors merit further experimentation in future work, but it is clear that critical balances exist where information-sharing becomes an impactful control against systemic risk. We can observe that there is a time differential on the effectiveness of information-sharing. If the prey are becoming infected and reaching a peak extremely quickly (due to high propagation, high number of predators, or both), then information-sharing makes little difference. For our model of information-sharing, we can reason about the conditions under which information sharing will be effective against propagating ransomware (and viruses more broadly) through the following relation between the number of prey, number of attackers, attacker bandwidth, and propagation bandwidth:

- Assume propagation is always to new prey (that have not been previously infected); i.e., look at “worst case” for propagation speed—giving an upper bound on the information-sharing speed needed. Also assume no prey are recovering (again, a worst case).
- $n_a$  is number of attackers,  $s_a$  is attacker bandwidth,  $s_p$  is propagation bandwidth,  $n_y$  is number of prey,  $t_i$  is threat intelligence time threshold (assume that there is a time threshold where threat intelligence comes into effect and prey patch).
- Then the number of prey compromised at time  $t$  is  $C(t) = n_a * s_a * s_p * t$ .
- This becomes saturated (all prey compromised) when  $C(t) = n_y = n_a * s_a * s_p * t$ .
- Therefore, it is necessary that  $t_i < t = \frac{n_y}{n_a * s_a * s_p}$  for threat intelligence sharing to have any impact on the maximum number of prey compromised.

This relation could be refined using more granular data on factors such as the time taken by victims to recover, if such data were available. The relation is reflected in the simulation results: Figures 11 and 12 show that the maximum number of prey compromised and the speed with which this maximum is reached are reduced as the number of predators and the propagation rate are reduced; “weaker” threat-intelligence sharing (with a higher time threshold) could therefore still reduce the maximum number of prey compromised.

We can approximate the **Return on Security Investment (ROSI)** from participating in the **cyber threat intelligence (CTI)** sharing community. We initially consider several costs to participate in the sharing community, including membership cost, operational costs, data privacy loss, and reputational damage. We neglect data-privacy loss, as this can be reduced applying data-privacy techniques, and thus reputational damage is also neglected. Therefore, we assume the membership and operational costs as investments. According to H-ISAC [7], there are seven membership tiers that depend on the organisation's revenue, ranging from \$3,000 to \$60,000 annually. However, Sophos reported the average loss for an organisation to rectify a ransomware attack in 2020, considering all related costs, i.e., recovery cost, was \$1.85 million [9]. Thus, given that the investments for

participating in the information-sharing community are several orders of magnitude smaller than the average losses caused by ransomware, the ROSI is relatively positive.

#### 7.4 Reflections on the Modelling Approach

We believe that using a compartment model in this research is advantageous, since it allows us to track the states of prey and therefore identify scenarios in which widespread failures (prey compromise and recovery) are observed across prey (indicating systemic risk). Given the large number of probabilities and functions of the model, dependent on state, the complexity was too great to feasibly allow analysis based on probability theory.

We framed the model as a compartment-based approach to modelling predator-prey interactions. A key aspect of predator-prey models is the presence of a stable oscillation between the populations of predators and prey. This can be represented by the **Lotka-Volterra (L-V)** equations, which describe both the rate of change in the size of the predator population and the rate of change in the size of the prey population as functions of the number of both predators and prey (i.e., the sizes of the two populations are co-dependent) [17]. The simulations presented in this article do not present the oscillations that are characteristic of predator-prey models, but tend towards a stable fixed-point solution that is characteristic of compartmental models.

We have taken inspiration from predator-prey modelling in our representation of the attacker and defender population, allowing us to consider factors inspired by predator-prey interactions such as proximity; but we have not presented an L-V model of predator-prey interactions. The model of predators is too simple to yield L-V oscillations, particularly since we have not introduced any function moving inactive predators to the active state. In this article, the investigation of a richer prey model has enabled valuable analysis of the validity of the model. We anticipate that the model presented in this article provides a foundation on top of which we can introduce a more complex model of the predator lifecycle. A next step in this research will be to enrich the predator model, including modelling predators' mutation to use different tactics and weapons or target different prey under certain conditions; modelling of realistic predator motivations for targeting or ceasing to target prey; and modelling of the creation and sharing of different types of weapons among the predator community. We anticipate that an enriched model of the predator lifecycle may result in L-V oscillations indicating dependence of the growth of each population on the size of the other; exploring this is an avenue for future work.

#### 7.5 Limitations and Data-collection Requirements

Certain elements of our modelling needed to be based on best estimates: In assigning some of the parameter values and probabilities, we found that data did not exist at a sufficiently granular level to support the precise assignment of values.

In Section 4.5.1, we document our assignment of values to function probabilities based on the available data and necessary inferences. In Section 3, we also highlighted a number of assumptions we needed to make on the behaviours of ransomware attackers and defenders. We believe that our justifications for assigning values are sufficiently robust to support our high-level conclusions about systemic-risk behaviours and dynamics and the impact of defensive policies. However, there is a need for data-collection and analysis efforts to establish a robust basis for building accurate models in this space. Some of the key data-collection needs we have identified through this work include:

- The incident-response actions taken by organisations in response to attacks (both ransomware and more broadly) and the effectiveness of these responsive actions.
- The effectiveness of organisations' protective capabilities against attacks (i.e., statistics on attacks prevented before infecting organisations) and variations in effectiveness.
- The impact of various conditions on organisations' patching practices (e.g., frequency of patching following receipt of threat intelligence or post-compromise).

- The speed with which tools for fixing ransomware's impacts are made available, their effectiveness, and usage by organisations.
- The size of coordinated attack campaigns (e.g., the volume of attackers simultaneously launching ransomware attacks such as WannaCry) and the effect of **Ransomware-as-a-Service (RaaS)** on these volumes (ransomware sold as a distribution kit on the dark web, which can expand the range of possible attackers, since adversaries with less technical skill are able to leverage the toolkits to attack [50]).
- The behaviours of large information-sharing communities, including the relationship between the level of information shared and the likelihood of community members taking action (such as patching and improving protection capability).
- The behaviours of ransomware groups in response to a lack of ransom payment, which might include ceasing to launch ransomware attacks, evolving their tactics to using different types of ransomware or targeting different victim populations.

## 8 CONCLUSION AND FUTURE WORK

In this article, we have represented ransomware that propagates via the Internet through a compartment-based approach to modelling predator-prey interactions, and we have shown how this can be used to understand how various risk controls might help address this form of systemic risk. Our simulations exploring the effectiveness of three types of controls against systemic risk produced results that aligned with our expectations, showing the accuracy of the model in representing the relevant dynamics. These results gave insights that enabled us to reason about the factors that impact on the effectiveness of these controls; for example, the time differential governing the effectiveness of information sharing in reducing the spread of a propagating virus.

We believe that this modelling approach could be extended as future work to explore a broader range of attack types, attacker behaviours, characteristics of the victim population, and risk-mitigation approaches and their impacts on systemic risk.

These extensions include exploring the effects of further predator tactics by incorporating multiple ransomware variants and mutations alongside other forms of attack; further exploring the targeting of attacks by predators (e.g., the relative importance of factors such as sector and revenue in determining “proximity”); and exploring the impacts of predator tactics such as payment pressure. Extensions could also include more detailed study of the effect of various parameters of community behaviours such as information sharing; for example experimenting with variations in data quality and with the effect of multiple information-sharing communities with different characteristics co-existing (representative of sectoral information-sharing communities). Running sensitivity analyses of the model to factors such as individual organisations' protection, detection, and response capability, and quality of information shared between organisations, could support reasoning about the importance of these factors for mitigating the systemic risk from ransomware.

Additional risk-mitigation approaches such as cloud-based backups might be explored, in particular their impact on systemic risk (for example, many recent ransomware attacks include data in the public cloud [31], and this risk-mitigation approach might in fact create a new target for attackers to impact many dependent organisations at once). The approach could also be extended to take into account further systemic-risk factors such as the upstream and downstream dependencies of organisations (noting recent supply-chain attacks such as the SolarWinds hack [4]) and a lack of diversity of technology and providers. Extending the model to represent the actions of law enforcement would provide an opportunity to explore the impact of various law-enforcement policies in terms of both deterring attackers and influencing the actions of prey. Finally, the model could be expanded to incorporate monetary values, enabling calculation of the expected financial impact of various defensive behaviours (e.g., time to patch and the various recovery strategies).

We have noted the need for more robust data on a number of factors. Future work should seek to strengthen the evidence base for attacker and victim behaviours, which could support research into a wide range of

cybersecurity issues, including the modelling of predator and prey behaviours in the context of systemic cybersecurity risk. Key examples include robust evidence on organisations' use of defensive controls and response to attacks, and on attackers' targeting of organisations. Data is also needed to support research into the economics of ransomware and predator dynamics in response to payment and non-payment of ransoms by the population of victim organisations. For example, we might anticipate that predators who are paid ransoms might use the funds to develop a greater capacity over time, while those who are not paid might cease attacking or switch to using other attack methods or ransomware variants. In light of the difficulty of collecting some of the necessary data, the experience of experts might also be drawn on to refine and validate models; approaches such as a Delphi study of experts would be a valuable next step.

## REFERENCES

- [1] 2017. *Midyear Security Roundup: The Cost of Compromise - Security Roundup*. Technical Report. Trendmicro. Retrieved from <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-cost-of-compromise>.
- [2] 2020. *2020 Cyberthreat Defense Report*. Technical Report. Cyber Edge Group.
- [3] 2020. *The 2020 Ransomware Resiliency Report*. Technical Report. Veritas.
- [4] 2020. *Dealing with the SolarWinds Orion Compromise*. Technical Report. National Cyber Security Centre (NCSC).
- [5] 2020. *Mitigating Malware and Ransomware Attacks*. Technical Report. National Cyber Security Centre (NCSC).
- [6] 2020. *Threat Landscape 2020—Ransomware*. Technical Report. European Union Agency for Cybersecurity (ENISA).
- [7] 2021. *H-ISAC Membership*. Technical Report. H-ISAC. <https://h-isac.org/membership-account/join-h-isac/>.
- [8] 2021. *No More Ransom Project*. Retrieved from <https://www.nomoreransom.org/en/index.html>.
- [9] 2021. *The State of Ransomware 2021*. Technical Report. Sophos.
- [10] 2022. *The State of Ransomware 2022*. Technical Report. Sophos.
- [11] 2022. *Systemic Cybersecurity Risk and Role of the Global Community: Managing the Unmanageable*. Technical Report. World Economic Forum.
- [12] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* 74 (2018), 144–166.
- [13] Randi Eitzman, Alex Berry, and Josh Homan. 2017. *WannaCry Malware Profile*. Retrieved from <https://www.mandiant.com/resources/wannacry-malware-profile>.
- [14] Pranshu Bajpai, Aditya K. Sood, and Richard Enbody. 2018. A key-management-based taxonomy for ransomware. In *APWG Symposium on Electronic Crime Research (eCrime'18)*. IEEE, 1–12.
- [15] David Bisson. 2017. *WannaCryptor Ransomware Strikes NHS Hospitals, Telefonica, and Others*. Retrieved from <https://www.tripwire.com/state-of-security/latest-security-news/wannacryptor-ransomware-strikes-nhs-hospitals-telefonica-and-others/>.
- [16] Abhijit Bose and Kang G. Shin. 2006. On mobile viruses exploiting messaging and Bluetooth services. In *SecureComm and Workshops*. IEEE, 1–10.
- [17] Fred Brauer and Carlos Castillo-Chavez. 2012. *Mathematical Models in Population Biology and Epidemiology*, Vol. 2. Springer.
- [18] Ross Brewer. 2016. Ransomware attacks: Detection, prevention and cure. *Netw. Secur.* 2016, 9 (2016), 5–9.
- [19] Elisa Canzani. 2016. Modeling dynamics of disruptive events for impact analysis in networked critical infrastructures. *ISCRAM Conference* (2016).
- [20] Elisa Canzani. 2017. *Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures*. Ph.D. Dissertation. Munich University. Retrieved from <https://athene-forschung.unibw.de/doc/122159/122159.pdf>.
- [21] Elisa Canzani and Stefan Pickl. 2016. Cyber epidemics: Modeling attacker-defender dynamics in critical infrastructure systems. In *Advances in Human Factors in Cybersecurity*, Denise Nicholson (Ed.), Vol. 501. Springer International Publishing, Cham, 377–389. DOI: [https://doi.org/10.1007/978-3-319-41932-9\\_31](https://doi.org/10.1007/978-3-319-41932-9_31)
- [22] Edward Cartwright, Julio Hernandez Castro, and Anna Cartwright. 2019. To pay or not: Game theoretic models of ransomware. *J. Cybersecur.* 5, 1 (2019), tyz009.
- [23] Checkpoint. 2022. *Ransomware Recovery: How to Recover from Ransomware*. Retrieved from <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware-recovery-how-to-recover-from-ransomware/>.
- [24] Yugui Chu, Wanjuan Xia, and Zecheng Wang. 2019. A delayed computer virus model with nonlinear incidence rate. *Syst. Sci. Contr. Eng.* 7, 1 (2019), 389–406.
- [25] Jedidiah R. Crandall, Roya Ensafi, Stephanie Forrest, Joshua Ladau, and Bilal Shebaro. 2008. The ecology of Malware. In *Proceedings of the New Security Paradigms Workshop (NSPW'08)*. Association for Computing Machinery, 99–106. DOI: <https://doi.org/10.1145/1595676.1595692>
- [26] Sadie Creese, Jamie Saunders, Louise Axon, and William Dixon. 2020. *Future Series: Cybersecurity, Emerging Technology and Systemic Risk*. Technical Report. World Economic Forum.

- [27] Cybersecurity, Multi-state Information Sharing Infrastructure Security Agency, and Analysis Center. 2020. *Ransomware Guide*. Technical Report. Retrieved from [https://www.cisa.gov/sites/default/files/publications/CISA\\_MS-ISAC\\_Ransomware%20Guide\\_S508C\\_.pdf](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf).
- [28] Tooska Dargahi, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi, and Loris Benedetto. 2019. A cyber-kill-chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hack. Techniq.* 15, 4 (2019), 277–305.
- [29] Shahab Ud Din, Zaheer Masood, Raza Samar, Khalid Majeed, and Muhammad Asif Zahoor Raja. 2017. Study of epidemiological based dynamic model of computer viruses for sustainable safeguard against threat propagations. In *14th International Bhurban Conference on Applied Sciences and Technology (IBCAST'17)*. IEEE, 434–440.
- [30] Jian Ding, Zizhen Zhang, and Xuemin Chen. 2019. A delayed predator-prey model for worm propagation in computer systems. In *IEEE 16th International Conference on Networking, Sensing and Control (ICNSC'19)*. IEEE, 41–45.
- [31] Cybersecurity Federal Bureau of Investigation and Australian Cyber Security Centre National Cyber Security Centre Infrastructure Security Agency, National Security Agency. 2022. *Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat of Ransomware*. Technical Report. Retrieved from <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>.
- [32] FireEye. 2020. *Breaking in After Hours: Ransomware Trend Intelligence*. Retrieved from <https://vision.fireeye.com/editions/07/07-breaking-in-after-hours.html#>.
- [33] European Union Agency for Cybersecurity (ENISA). 2018. *Information Sharing and Analysis Center (ISACs) - Cooperative Models*. Technical Report. Retrieved from <https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models>.
- [34] Richard Ford, Mark Bush, and Alexander Bulatov. 2006. Predation and the cost of replication: New approaches to malware prevention? *Comput. Secur.* 25, 4 (June 2006), 257–264. DOI : <https://doi.org/10.1016/j.cose.2006.02.002>
- [35] Sean P. Gorman, Rajendra G. Kulkarni, and Laurie A. Schintler. 2004. A predator prey approach to the network structure of cyberspace. *Winter International Symposium on Information and Communication Technologies (WISICT)*, ACM, 1–6.
- [36] A. Gupta and D. C. DuVarney. 2004. Using predators to combat worms and viruses: A simulation-based study. In *20th Annual Computer Security Applications Conference*. 116–125. DOI : <https://doi.org/10.1109/CSAC.2004.47>
- [37] Alex Hern and Samuel Gibbs. 2017. *What Is WannaCry Ransomware and Why Is It Attacking Global Computers?* Retrieved from <https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20>.
- [38] Herbert W. Hethcote. 1989. Three basic epidemiological models. In *Applied Mathematical Ecology*, S. A. Levin, Simon A. Levin, Thomas G. Hallam, and Louis J. Gross (Eds.), Vol. 18. Springer Berlin, 119–144. DOI : [https://doi.org/10.1007/978-3-642-61317-3\\_5](https://doi.org/10.1007/978-3-642-61317-3_5)
- [39] Gavin Hull, Henna John, and Budi Arief. 2019. Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Sci.* 8, 1 (2019), 2.
- [40] Alexandra Ioanid, Cezar Scarlat, and Gheorghe Militaru. 2017. The effect of cybercrime on Romanian SMEs in the context of WannaCry ransomware attacks. In *European Conference on Innovation and Entrepreneurship*. Academic Conferences International Limited, 307–313.
- [41] Jennifer T. Jackson and Sadie Creese. 2012. Virus propagation in heterogeneous Bluetooth networks with human behaviors. *IEEE Trans. Depend. Secure Comput.* 9, 6 (2012), 930–943.
- [42] Insurance Journal. 2021. Insurer AXA to Stop Paying for Ransomware Crime Payments in France. Retrieved from <https://www.insurancejournal.com/news/international/2021/05/09/613255.htm>.
- [43] Kaspersky. 2021. *Over Half of Ransomware Victims Pay the Ransom, but Only a Quarter See their Full Data Returned*. Retrieved from [https://www.kaspersky.com/about/press-releases/2021\\_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned](https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned).
- [44] Shambavi Sadayappan (Mandiant) Kathleen Metrick, Jared Semrau. 2020. *Think Fast: Time between Disclosure, Patch Release and Vulnerability Exploitation—Intelligence for Vulnerability Management, Part Two*. Retrieved from <https://www.mandiant.com/resources/time-between-disclosure-patch-release-and-vulnerability-exploitation/>.
- [45] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 3–24.
- [46] Brian Krebs. 2021. At least 30,000 U.S. organizations newly hacked via holes in Microsoft's email software. KrebsOnSecurity. <https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/>. Accessed February 10, 2023.
- [47] Munna Kumar, Bimal Kumar Mishra, and T. C. Panda. 2015. Effect of quarantine & vaccination on infectious nodes in computer network. *Int. J. Comput. Netw. Applic.* 2, 2 (2015), 92–98.
- [48] Munna Kumar, Bimal Kumar Mishra, and T. C. Panda. 2016. Predator-prey models on interaction between computer worms, Trojan horse and antivirus software inside a computer system. *Int. J. Secur. Applic.* 10, 1 (2016), 173–190.
- [49] Martin Lee, Warren Mercer, Paul Rascagneres, and Craig Williams. 2017. Player 3 Has Entered the Game: Say Hello to “WannaCry.” Retrieved from <http://blog.talosintelligence.com/2017/05/wannacry.html>.
- [50] Mark Loman. 2019. *How Ransomware Attacks*. Technical Report. Sophos.
- [51] Sandip Mandal, Ram Rup Sarkar, and Somdatta Sinha. 2011. Mathematical models of malaria-a review. *Malaria J.* 10, 1 (2011), 1–19.

- [52] Lockheed Martin. 2011. *Cyber Kill Chain*. Retrieved from <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
- [53] Wojciech Mazurczyk and Elżbieta Rzeszutko. 2015. Security—A perpetual war: Lessons from nature. *IT Profess.* 17, 1 (Jan. 2015), 16–22. DOI : <https://doi.org/10.1109/MITP.2015.14>
- [54] Siyakha N. Mthunzi and Elhadj Benkhelifa. 2017. Survivability analogy for cloud computing. In *IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA'17)*. 1056–1062. DOI : <https://doi.org/10.1109/AICCSA.2017.219>
- [55] Siyakha N. Mthunzi, Elhadj Benkhelifa, Tomasz Bosakowski, and Salim Hariri. 2019. A bio-inspired approach to cyber security. In *Machine Learning for Computer and Cyber Security* (1st ed.), Brij B. Gupta and Michael Sheng (Eds.). CRC Press, Boca Raton, FL, 75–104. DOI : <https://doi.org/10.1201/9780429504044-4>
- [56] BBC News. 2021. Ransomware: Should Paying Hacker Ransoms Be Illegal? Retrieved from <https://www.bbc.co.uk/news/technology-57173096>.
- [57] Bao Nguyen. 2017. Modelling cyber vulnerability using epidemic models. In *Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*. SCITEPRESS - Science and Technology Publications, Madrid, Spain, 232–239. DOI : <https://doi.org/10.5220/0006401902320239>
- [58] National Institute of Standards and Technology (NIST). 2018. *Cyber Security Framework (CSF) v1.1*. Technical Report. Retrieved from <https://www.nist.gov/cyberframework>.
- [59] Unit 42 Palo Alto. 2022. *Ransomware Threat Report*. Technical Report. Retrieved from [https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html?utm\\_source=google-rapp-amer-rapp&utm\\_medium=paid-search&utm\\_campaign={campaign}&utm\\_content=591939886994-c&utm\\_term=ransomware%202021&sfdc=7014u000001hKM8AAM&\\_bt=591939886994&\\_bm=e&\\_bn=g&gclid=Cj0KCQjw1ZeUBhDyARIsAOzAqQIx2E0MsGF519Z7\\_-vT8UzCjFcQKmlGny0nEAs\\_duubZzRCl\\_6CrQaAuAQEALw\\_wcB](https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html?utm_source=google-rapp-amer-rapp&utm_medium=paid-search&utm_campaign={campaign}&utm_content=591939886994-c&utm_term=ransomware%202021&sfdc=7014u000001hKM8AAM&_bt=591939886994&_bm=e&_bn=g&gclid=Cj0KCQjw1ZeUBhDyARIsAOzAqQIx2E0MsGF519Z7_-vT8UzCjFcQKmlGny0nEAs_duubZzRCl_6CrQaAuAQEALw_wcB).
- [60] Jonathan Pan and Chun Che Fung. 2012. An agent-based model to simulate coordinated response to malware outbreak within an organisation. *Int. J. Inf. Comput. Secur.* 5, 2 (2012), 115–131.
- [61] Norman Pendegraft. 2017. Predator-prey/obligate mutualism in information system security and usage. *J. Inf. Technol. Theor. Applic.* 18, 1 (2017), 42.
- [62] Home Office Cyber Security Programme. 2019. *Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts*. Technical Report. Retrieved from <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf>.
- [63] Hao Qiang and Wenlian Lu. 2018. A note on dependence of epidemic threshold on state transition diagram in the SEIC cybersecurity dynamical system model. In *Science of Cyber Security (Lecture Notes in Computer Science)*, Feng Liu, Shouhuai Xu, and Moti Yung (Eds.). Springer International Publishing, Cham, 51–64. DOI : [https://doi.org/10.1007/978-3-030-03026-1\\_4](https://doi.org/10.1007/978-3-030-03026-1_4)
- [64] Angel Martín del Rey. 2015. Mathematical modeling of the propagation of malware: A review. *Secur. Commun. Netw.* 8, 15 (2015), 2561–2579. DOI : <https://doi.org/10.1002/sec.1186>
- [65] IBM Security. 2022. *Definitive Guide to Ransomware 2022*. Technical Report. Retrieved from <https://www.ibm.com/downloads/cas/EV6NAQR4>.
- [66] Daniele Sgandurra, Luis Muñoz-González, Rabih Mohsen, and Emil C. Lupu. 2016. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint arXiv:1609.03020* (2016).
- [67] Rhythima Shinde, Pieter Van der Veeken, Stijn Van Schooten, and Jan van den Berg. 2016. Ransomware: Studying transfer and mitigation. In *International Conference on Computing, Analytics and Security Trends (CAST'16)*. IEEE, 90–95.
- [68] Christian Sillaber, Clemens Sauerwein, Andrea Musmann, and Ruth Breu. 2016. Data quality challenges and future research directions in threat intelligence sharing practice. In *ACM Workshop on Information Sharing and Collaborative Security*. 65–70.
- [69] Camelia Simoiu, Joseph Bonneau, Christopher Gates, and Sharad Goel. 2019. “I was told to buy a software or lose my computer. I ignored it”: A study of ransomware. In *15th Symposium on Usable Privacy and Security (SOUPS'19)*.
- [70] Luke Somerville. 2017. WannaCry Post-outbreak Analysis. Retrieved from <https://www.forcepoint.com/blog/x-labs/wannacry-post-outbreak-analysis>.
- [71] Peter Mackenzie (Sophos). (2021). *The Top 10 Ways Ransomware Operators Ramp Up the Pressure to Pay*. Retrieved from <https://news.sophos.com/en-us/2021/10/28/the-top-10-ways-ransomware-operators-ramp-up-the-pressure-to-pay/>.
- [72] Nicole Perlroth (New York Times). 2021. *A Rare Win in the Cat-and-Mouse Game of Ransomware*. Retrieved from <https://www.nytimes.com/2021/10/24/technology/ransomware-emsisoft-blackmatter.html>.
- [73] The New York Times. 2021. Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers. Retrieved from <https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>.
- [74] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. 2019. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* 87 (2019), 101589.
- [75] Alex Wilner, Anna Jeffery, Jacqueline Lalor, Kathleen Matthews, Krystene Robinson, Alexandra Rosolska, and Catherine Yorgoro. 2019. On the social science of ransomware: Technology, security, and society. *Comparat. Strat.* 38, 4 (2019), 347–370.
- [76] Wired. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

- [77] Lena Yuryna Connolly, David S. Wall, Michael Lang, and Bruce Oddson. 2020. An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *J. Cybersecur.* 6, 1 (2020), tyaa023.
- [78] Kim Zelonis. 2004. *Avoiding the Cyber Pandemic: A Public Health Approach to Preventing Malware Propagation*. Ph.D. Dissertation. Carnegie Mellon University Heniz School (MSISPM).
- [79] Zizhen Zhang and Limin Song. 2017. Dynamics of a delayed worm propagation model with quarantine. *Adv. Differ. Equat.* 2017, 1 (2017), 1–13.

Received 30 November 2021; revised 21 November 2022; accepted 15 December 2022