COORDINATE: A model to analyse the benefits and costs of coordinating cybercrime

Tom Meurs[1]*, Marianne Junger[1], Abhishta Abhishta[1], Erik Tews[1], and Emma Ratia[2]
[1]University Twente, Enschede, The Netherlands
t.w.a.meurs@utwente.nl, m.junger@utwente.nl, s.abhishta@utwente.nl, e.tews@utwente.nl
[2]Dutch National Police, Driebergen, The Netherlands
emma.ratia@politie.nl

Abstract

Recent leaks (such as Conti) have provided greater insights on the working of cybercriminal organisations. Just like any other business, these malicious actors strategically manage their processes in order to maximise their revenues. Coordinating different types of cybercrimes as part of a single attack campaign provides another opportunity to these criminal groups to improve the efficiency of their attacks. To investigate the promise of this "coordination" between cybercrimes in improving the financial gains realised by cybercriminals, we take a two-step approach. First, we perform a bibliometric analysis of past scientific literature discussing the concept of "coordination" w.r.t to cybercrime. Second, as a case study, analysing the attack chains of DDoS, phishing and ransomware attacks, we identify vantage points for potential coordination from an attacker's perspective. Based on our findings, we propose a model (COORDINATE) to identify the types of potential cybercrime "coordinations". COORDINATE considers three relevant types of coordination: direct collaborated coordination, indirect collaborated coordination, and opportunistic coordination. Given the advantages of coordinated attacks, our results suggest that one crime may provide opportunities for the next one. Coordinated attacks will become more prevalent, and that we may witness the development of a dynamic that leads to more online crime.

Keywords: Coordination, DDoS, Phishing, Ransomware

1 Introduction

Cybercriminals can achieve greater success in their endeavours by using a coordinated set of attack techniques in their strategy [1]. Maastricht University in the Netherlands was struck by a serious ransomware attack which led to attackers gaining access to the computers on December 23rd, 2019. The criminals obtained initial access by sending two phishing emails, where two employees clicked on the attachment [2]. Subsequently, the university decided to pay a ransom of 197,000 euros to get access to the data encrypted by criminals. However, not all victims of ransomware pay ransom when the demands are first made. For instance, when Glen Dimplex Home Appliances got attacked in October 2020 and they paid the ransom only when the attackers pressured the company by performing a Distributed Denial-of-Service (DDoS) attacks [3]. These examples show that some attacks that at first sight may appear different attack events, but may be part of the same attack event. According to [4], these type of attack events are among the most aggressive and prevalent. We define coordination as *the use of different attacks or crimes for a single attack event*. Understanding coordination is essential to find effective and successful prevention strategies against cybercrime.

Most work on coordination of cyberattacks from a computer science perspective [5], focus on attack coordination and orchestration. To the best of our knowledge, this is mostly theoretical and does not

*Corresponding author: Department of Industrial Engineering and Business Information Systems, University of Twente, The Netherlands, Tel: +31-534-898-289

focus on specific cybercrimes. Another part of research literature focuses on the cooperation of criminal actors from an economical [6, 7] or criminological [8] perspective. However, in our view, collaboration and cooperation are different from coordination. As suggested previously, coordination is *the use of different attacks or crimes for a single attack event*. On the contrary, collaboration is *when a group of malicious actors work on a shared objective*. For example, when malware developers and black-hat pentesters working together within a ransomware group [9]. Cooperation is *when a group of malicious actors are working together to help accomplish the goal of one of the groups*. Cooperation is a subset of collaboration. For example, a phishing group helping a ransomware group to get access to a network to install their ransomware. Collaboration and cooperation focus on the relationship between actors, whereas we are interested in the relationship between crimes. Also, we would like to stress that collaboration and cooperation are not mutually exclusive: within a single attack event, both can occur independently of each other.

Although coordinated attacks have been described by cybersecurity companies and blogs [10, 11, 12], to our knowledge no previous scientific research has systematically investigated the coordinated attacks from an attackers perspective using specific cybercrimes. Additionally, in this study we will argue that coordinated attacks could be more beneficial for the attacker and more severe for the victim than regular types of attack, and that the evolving cybercrime ecosystem will facilitate coordinated attacks in the future. Therefore, this study will focus on coordinated attack events.

We explore coordinated attack events by performing a systematic literature review of coordinated cyberattacks using a bibliometric mapping. Subsequently, we use that information to perform a case study on the coordination of three relatively frequent cybercrimes: DDoS, phishing and ransomware attacks. Previous research has focused on the understanding and prevention of these individual crimes and not their interaction [13, 14, 15]. We illustrate cases of coordination of DDoS, phishing and ransomware as described by the security industry and identify possible vantage points for attackers to coordinate these attacks. Subsequently, we propose COORDINATE: a model to describe different types of coordinated attacks and the benefits and costs for an attacker to decide to coordinate an attack.
Overall, our work focuses on addressing the following research questions:

(i) What is the current state of literature on the coordination and collaboration of cybercrimes?

(ii) What are the costs and benefits for an offender to decide to perform a coordinated attack or not?

The contributions of this work are twofold:

1. A bibliographic mapping of previous academic literature on coordination and collaboration of cybercrimes;

2. Second contribution can be divided into three parts:

   2.a. Introduce a case study of coordinating DDoS, phishing and ransomware and identify potential vantage points for attackers to coordinate these attacks;

   2.b. Identify recent developments in the cybercrime ecosystem and analyse, why they facilitate coordinated attacks;

   2.c. Integrating points 1 and 2.a. into a conceptual model COORDINATE. COORDINATE describes four types of coordination and provides testable hypothesis of the pros and cons of coordination from the criminal's perspective.

The remainder of this paper is organised as follows. First, we elaborate in Section 2 on previous academic literature on coordination and cooperation of cybercrimes. We introduce in Section 3 a case

study: the coordination of DDoS, phishing and ransomware. We explain in Section 4 how the evolving cybercrime ecosystem facilitates the coordination of cybercrimes in the future. Considering these points, we deduce a hypothetical model to describe different types of coordinated attacks and suggest testable predictions for future empirical studies. Finally, in Section 5 we summarise our key findings.

2 Bibliometric mapping

In this section, we discuss the results of bibliometric analysis of previous academic literature on "coordination" and "collaboration" in relation to cybercrime. First, we discuss the methodology used to perform the bibliometric mapping. Then we present our key findings.

To find the relevant keywords to search for academic literature that discussed "cooperation" and "coordination" with relation to cybercrime, we follow the method described by [16]. They suggest a four step protocol:

(i) Decompose the research question into individual elements.

(ii) Obtain key-words from primary studies.

(iii) Identify synonyms for the main terms.

(iv) Construct search strings using Boolean "AND" to join the main terms and "OR" to include synonyms.

Afterwards, the boolean search string was used to query the literature database Scopus. Subsequently, the literature from the field of mathematics, medical, physics and astronomy sciences were excluded as they are not relevant for studying cooperation and coordination of cybercrimes. We use VOS viewer [17] to identify clusters within resulting literature. We use bibliometric coupling (a measure that represents the number of references shared between two publications) to identify these clusters. Hence, publications within the same cluster, have a substantial overlap in the reference list. We analyse the abstracts of each cluster by using the wordcount of each word in the abstract. Using the top 20 most occuring words within the abstracts of a cluster we identify the clusters which are most relevant to concepts "coordination" and "collaboration" of cybercrimes and cybercriminals. If synonym of these concepts were present in these 20 words we further investigate the content of these clusters. The studies within these clusters were compared to our research objective as described in Section 1.

Using the methodology as described above, the main terms of our query were cybercrime and cyberattack, coordination, collaboration, business model and cooperation. We search Scopus database using the following query:

('cyber') AND ('crime' OR 'attack') AND ('coordinat*' OR 'collabora*' OR 'business model' OR 'cooperat*')

Using the Scopus database we found 2341 articles as a result of this query. We excluded publications from the fields of mathematics, medical sciences, physics and astronomy and as a result obtain 1762 articles. The yearly distribution of these publications are shown in Figure 2.

These 1762 articles were used for the bibliometric mapping in VOS Viewer. As described above, we used bibliometric coupling as a measure to identify clusters of publications related to a similar topic. All the identified clusters are shown in Figure 1. Table 1 shows the number of studies we found for each cluster. Using the 20 most occurring words of each cluster, we find the clusters most relevant to our study. We identify clusters 1, 7, 9, 10 and 11 as related to concepts of coordination and/or collaboration

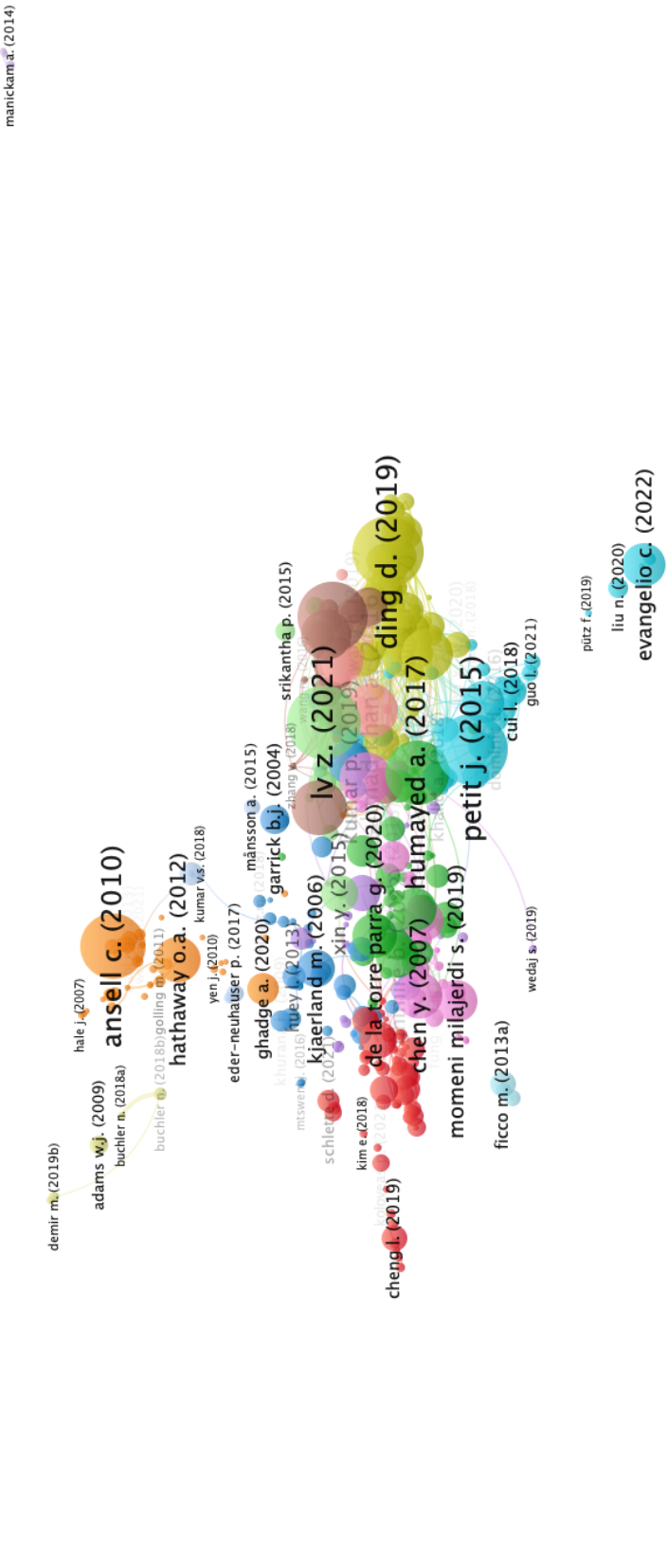

Figure 1: Clusters of selected literature. The different colors represent the different clusters of academic literature on coordination of cybercrimes.

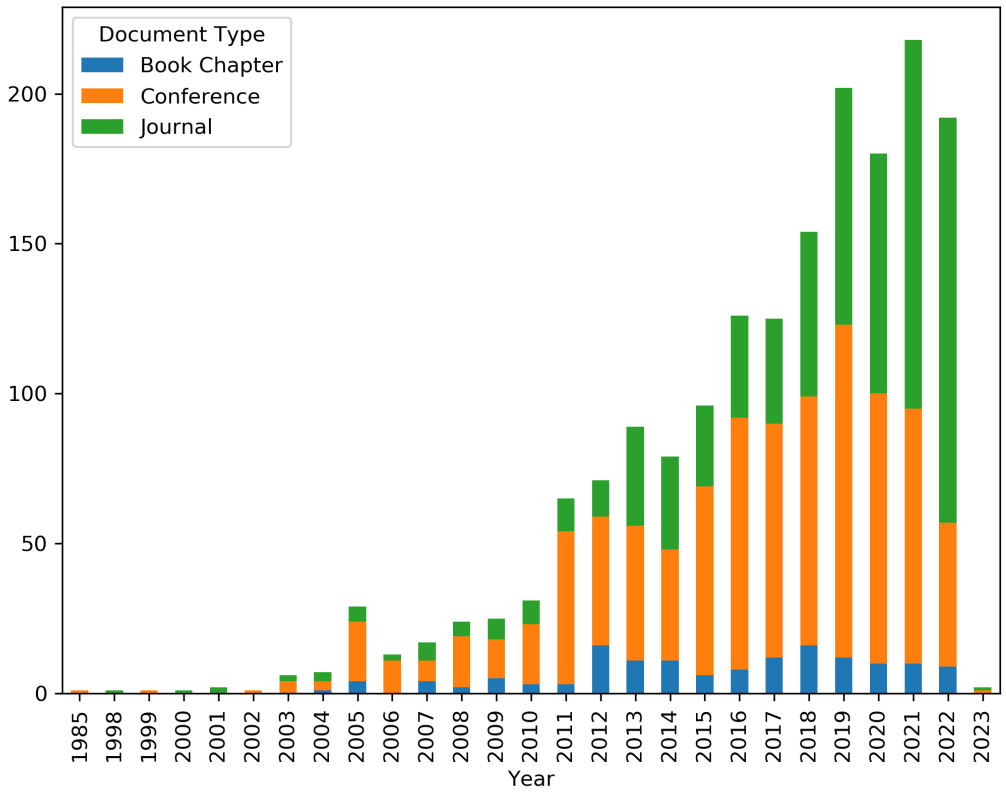

Figure 2: Yearly #publications indexed by Scopus.

Cluster	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of studies	64	61	44	42	36	33	31	25	24	32	26	17	15	13	7	2

Table 1: Number of studies per cluster found in VOS viewer with the extracted studies from Scopus.

of cybercrimes. We analyse the studies in each of these clusters to find the connection of these clusters with concepts of coordination/collaboration.

Cluster 1: Keywords: network, framework, attack, security, data. This cluster describes studies were defensive systems coordinate to deter cybercrime. For example, [18] studies the collaboration of different IDPS to detect botnets. [19] develops a honeypot for collaborative defense against distributed attacks of interconnected attackers. Unfortunately, in this study the authors do not explain what distributed attacks of interconnected attackers look like.

Cluster 7: Keywords: vehicle, system, attack, safety, communication. This cluster describes coordination of different systems in a vehicle or several (autonomous) vehicles to defend against cyberattacks. For example, [20] and [21] study cyberattacks against connected autonomous vehicles.

Cluster 9: Keywords: attack, system, power, based, grid. This cluster describes coordinated attacks on a power grid system. The focus is on coordination of the same type of cyberattack. For example, [22] explores distributed smart grid attack strategies to destabilise power system components. The

(a) 20 most occurring words in Cluster 10.

(b) 20 most occurring words in Cluster 11.

Figure 3: Word cloud of 20 most occurring words in abstracts of Cluster 10 (a) en Cluster 11 (b).

authors consider the objective of the attacker to disrupt the power system by taking control over breakers and coordinating attacks. Subsequently, a strategy is formulated for the opponent to leverage variable structure system theory to attack.

Cluster 10: Keywords: attack, network, model, security, attacker. This cluster describes different cyberattack models, coordinated and collaborated attacks. For example, [23] use a game theoretic approach to model the dynamic behaviour between attacker and defender. The authors argue that each actor adjust his strategy based on costs, potential gain and/or damage and effectiveness of participating the opponent's strategy. [24] develops a canonical model for cyberoperation by advanced attackers. They assume an isolated attack by an individual attacker of homogeneous group. [25] constructs a detection method which can recognise coordinated attacks, by building a 'requires/provides' model. The authors test their model on the multi-stage attack of the Zeus botnet. [26] presents a high-level framework of defending against a cyberattack collaborated by interconnected attackers. The framework consists of five attributes of a coordinated attack: time-aspect, space-aspect, effect of an attack, information change during an attack and the privacy aspect.

Cluster 11: Keywords: system, attack, proposed, model, cyber-physical. Coordination of power grid systems. For example, [27] considers cyber-physical coordinated attacks against power grid and how to formulate a defensive strategy to defend. [28] develops a estimation-based anomaly detection method to defend against cyber-physical smart grid systems. With cyber-physical translates to both cyber as physical security of power systems. This cluster seems highly related to cluster 9.

We can conclude that cluster 10 is most interesting considering the objectives from Section 1. Most studies out of cluster 10 are theoretical or consider high-level frameworks of coordinated attacks [23, 26], as for example the canonical model for cyberoperations by advanced attackers [24]. In this study take a different approach: we focus on the costs and benefits of conducting coordinated attacks compared to isolated attacks from the attackers perspective. In the next sections based on a case study we argue the importance to not only consider how coordinated attacks are performed, but also why attackers have incentives to do so.

3 Case Study: Coordinating DDoS, Phishing and Ransomware attacks

In this section we present a case study of coordinating DDoS, phishing and ransomware attacks. First, we performed a small literature review on whether examples of coordination of these three crimes have been studied. In Section 3.1 the methodology of finding relevant literature is examined. On the basis of this literature, we present a brief description of DDoS, phishing and ransomware in Section 3.2. In

Section 3.3 we examine possibilities of coordination of the specific crimes, based on the characteristics of the crimes themselves as described in Section 3.2. Finally, we consider the repetition of a specific crime as a specific case of coordination.

3.1 Methodology

To find specific use cases of coordination in combination with DDoS, phishing and ransomware in the academic literature, we use the following literature databases: Scopus and Web of Science. We have considered the articles/papers published in English language. Since the field of cybercrime is evolving very quickly and we were interested in the most recent modus operandi, we considered literature from the past four years (published since 2017). We also exclude any papers from the field of Medicine. For ransomware the keyword was 'ransomware', for phishing 'phishing' and for DDoS 'DDoS OR denial-of-service'. The results of the search and filtering are shown in Table 2.

Table 2: Search results of DDoS (DDoS OR denial-of-service), phishing and ransomware on different databases. Hits are the total number of hits with the query. Unique is the amount of unique articles from Scopus and Web of Science, where duplicates are removed and only attributed to Scopus.

Crime	DDoS		Phishing		Ransomware	
Database	Scopus	Web of Science	Scopus	Web of Science	Scopus	Web of Science
Hits	229	481	307	322	263	350
Unique	229	460	307	256	263	253

This resulted in 1765 articles, 689 for DDoS, 563 for phishing and 513 for ransomware. After removing the duplicates we selected articles based on the abstracts which described the modus operandi, victims, offenders, infrastructure or coordination. Articles concerning machine learning models or other automated defense strategies were excluded. This resulted in 244 articles: 97 of ransomware, 94 of phishing and 53 of DDoS. These articles were fully read and used for describing DDoS, phishing and ransomware in Section 3 and understanding the cybercrime ecosystem in Section 4. If the article referenced to other articles with relevant information about coordination, these other articles were also read, even if the article has been published before 2017. Finally, we add grey literature about coordination based on industry reports related to 'coordination cybercrime', 'DDoS phishing', 'DDoS ransomware', or 'phishing ransomware'. The end date of these queries was 13 September, 2021. This resulted in 16 articles from the security industry used in this paper. Based on these findings we first give a short description of the modus operandi of the specific crimes in the following section.

3.2 Overview DDoS, Phishing and Ransomware

Distributed Denial-of-service (DDoS) is a denial-of-service attack where attackers keep users from accessing a networked system, service, website, application, or other resource [29, 30]. A DDoS attack works by using all available network bandwidth or resources on a target network. Often this is done by using a botnet - entire networks of computers which are infected by malware and under control of a command and control (C&C) server, which is controlled by a botmaster [7]. Often, IoT devices are used for the botnet since they are hardly secured and available in abundance [31, 32]. Anyone with a website or network publicly accessible is prone to DDoS attacks. [30] indicate that 55% of DDoS attacks targeted financial services and web hosting companies. Other obvious targets are retail and e-commerce websites, whose revenue is highly dependent upon their website being available and responsive [33]. For more information about DDoS attacks we refer to [34, 33, 29].

Phishing is the sending of messages with the main objective to gather personal data of users [35, 36]. It is a popular method for stealing credentials, committing fraud and distributing malware. Phishing is based on social engineering: by using methods of persuasion the attacker tries to circumvent a victim's critical thinking and let him perform the action which the phisher wants to accomplish, like giving credentials or installing malware [35]. There are 3 types of targets for phishing: general/indiscriminate, semi-targeted and spear phishing [37]. Different types of phishing target different types of victims [38]: Indiscriminate phishing is when the attacker targets many unrelated victims hoping at least some will take the bait. Semi-targeted attacks focus on a specific organization or group. With spear phishing a specific individual (often C-level or IT-administrator) is targeted. For more information about phishing attacks we refer to [39, 40, 41].

Ransomware is a category of malicious software that prevents users from accessing their computing device resources by encrypting them [14]. Typically it prevents users from accessing their computing device or files, it shows a screen to provide a way for the victim to pay the ransom. Until the victim pays, the computing device is unusable. Often a deadline is mentioned and an anonymous payment method requested. Ransomware demands used to be typically between 300 to 2000 dollar per target, but is currently much higher [42, 43]. The attack targeting has shifted from individuals to companies [44, 42]. The reasons are twofold: First, targeting has shifted to the healthcare sector, government institutions, and education, because their data is most precious and they often pay high ransoms [45, 46]. Second, it is easier to infect a company than an individual. For more information about ransomware attacks we refer to [47, 42, 44].

3.3 Coordinating DDoS, Phishing and Ransomware attacks

(i) **Coordination of ransomware and phishing:** A first type of coordination is between ransomware and phishing. For ransomware to take place, an attacker has to gain access to a network or system. [46, 48, 42] indicate the importance of phishing to gain access to a network, which is than used to install ransomware and perform a ransomware attack. [42] mentions that email phishing accounts for 59% of initial access in ransomware attacks. [49] make the distinction between targeted and bulk ransomware. When the attack is indiscriminate, spam emails are a common way to attack. If the attack is targeted, (spear)phishing and the use of exploits are more typical.

Not only is phishing used to facilitate the installation of ransomware, also ransomware is increasingly used to indirectly steal credentials, which sometimes lead to more phishing [50, 51]. Another way ransomware leads to phishing is in which the content of the phishing email seems more credible by addressing a recent or on going ransomware attack. After the University of Maastricht faced a ransomware attack, it was targeted by a phishing campaign. The emails addressed the ransomware attack, and provided context and credibility to the malicious email [2].

A third way for ransomware to possibly lead to phishing was described by [50]. [50] studied different factors contributing to maximizing profit of a ransomware attack. Their conclusion was that combining ransomware with data-stealing is in general more profitable than ransomware without stealing the data, and that selling the stolen data is always more profitable than threatening to leak the data. Leaked data is often used for semi-targeted and spear-phishing [51]. Therefore this new method of stealing data during a ransomware attack provides additional opportunities for (targeted) phishing.

(ii) **Coordination of ransomware and DDoS:** A second type of coordination is ransomware and DDoS. Several studies indicate different ways to coordinate ransomware and DDoS. [52] mentions that DDoS is used as retribution for not being able to enter a network, to possibly install ransomware. Furthermore [53] and [54] mention that DDoS is increasingly used as leverage when

victims of a ransomware attack decide not to pay the ransom, as was mentioned in the introduction. As example, ransomware gangs like Avaddon group and SunCrypt are mentioned [54]. [55] actively scanned darknet forums and found ransomware actors to actively look for botmasters. This would suggest that ransomware actors do not use easy-to-buy booterservices, but want to possess their own infrastructure to conduct DDoS attacks. Additionally, REvil attackers told in an interview that they want to increase the use of DDoS during a ransomware attack, since victims are more willing to pay the ransom, according to the REvil actor [9].

DDoS is sometimes used to distract attention from a ransomware infection [56, 57]. In this context, an attack with the goal to distract from another attack will be defined as a smokescreen [11]. [57] mentions these smokescreens are done by doing sub-saturating DDoS attacks: low-bandwidth and short in duration (less than 5 minutes). This is done to prevent detection by DDoS mitigation systems. During those 5 minutes, IT staff is busy dealing with momentary network outages, whereas the criminals do automated scanning or penetration techniques to map the network and install the ransomware [57].

Besides these specific forms of coordination of ransomware and DDoS, a more fundamental similarity is that both ransomware and DDoS are basically a denial of resource [49, 58]. This indicates that ransomware and DDoS would only be coordinated if they attack different parts of a network, computer or system. For example, it would not make much sense to perform a DDoS attack on a public-facing server if it is already encrypted by ransomware.

(iii) **Coordination of phishing and DDoS:** A third type of coordination is between phishing and DDoS. Several articles describe cases of coordination between phishing and DDoS. Phishing is sometimes used to increase a botnet, which could be used for DDoS [7]. There are two ways phishing leads to an increased botnet. One way is to use credentials to automatically install malware [51]. Another is to send a email containing phishing and malware at the same time. Another possible link is the use of DDoS to either hide a phishing campaign, or make phishing emails seem more genuine by using it as a storyline or context [15, 59, 60].

The role of context in a phishing email was analysed by [61]. Students either got either an email about winning an I-Pad, or a course-related email. They found that 71.3 per cent of the participants who opened the course-related message also clicked on the simulated phishing link and 63.9 per cent submitted credentials. For the Ipad, these were respectively 5.9 and 3 per cent. They conclude that contextualized social engineering threats like course-related emails lead to victims overlooking cues of deception that normally would be caught in non-contextualized messages. The timing of phishing and DDoS was studied by [15]. They found there to be relatively more phishing emails send before and after a DDoS attack, compared to the baseline without DDoS attack. The authors claim this indicates a coordination of DDoS and phishing, although it could not be established whether this coordination was intended.

3.4 Campaigns and repeated attacks

It is worth noting that a form of coordination already exists for a long time within these three types of crimes:

(iv) **Multiple DDoS/phishing/ransomware attacks:** DDoS attacks often consists of multiple attacks. [29] analysed the probability of an attack. He found attacks to be relaunched on the same target less than 5 minutes after the end of the previous one is 58 %. 19 % of all attacks are part of a DDoS campaign of at least 5 consecutive attacks. These findings illustrate the effectiveness of

coordinating several DDoS attacks, which is defined as repeating attack [29]. This is also common for for many DDoS hacktivist, who work together to create a larger attack [62, 63].

Multiple phishing attacks: Bulk phishing can lead to spear-phishing (more targeted) [64]. An attacker sends the phishing emails first in bulk. When the attacker receives the credentials of the email-account, he or she will use this email-account to send new specifically targeted phishing emails to the contacts of the account. Since these emails originated from a trusted sender, more people are inclined to click on the link compared to phishing emails send in bulk [65]. Furthermore, phishing emails are often send in campaigns. [36] defined campaigns as sending a similar phishing email several times over a certain time span. Using campaigns is a cost-effective way to attack from the offender's perspective, since the attacker only needs to change the URL where the victim needs to click.

Multiple ransomware attacks: Ransomware could lead to more ransomware because of worm-like capabilities [48, 47, 42]. The ransomware could therefore infect an entire network automatically. This is the reason why WannaCry was so proliferate [42]. Another way different ransomware attacks are linked is because some high-value targets might be of interest to multiple ransomware actors. It happens that companies receive multiple ransomware attacks, encrypting their files multiple time. The only way to decrypt the files is when the ransomware actors cooperate [9].

Although campaigns and repeats could be considered a specific type of coordination, further analysis is outside the scope of this paper.

4 COORDINATE: the Cybercrime cOORDINATion modEl

Internet presents a global ecosystem that offers, among many other things, the tools, e.g., botnets, CaaS, crypto currencies, and an anonymous communication infrastructure, that enables the development and execution of attack chains [66, 67]. In this section, we describe how the recent development of tools and infrastructure within that ecosystem facilitates coordinated attacks and help explain the rise of reported coordinated attacks in Section 3. Subsequently, we propose COORDINATE, a new model of coordination and testable predictions to help analyse the costs and benefits of coordination for cybercriminals.

4.1 Development Tools and Infrastructure in Cybercrime Ecosystem

[68] analysed the cybercrime ecosystem by considering malware, bitcoins and darknet. We extend this research by briefly describing the evolution of underground forums and markets, cryptocurrencies, online anonymity and botnets. In essence, a cybercriminal wants to anonymously communicate with other cybercriminals (through underground forums and markets), anonymously receive and send money (with cryptocurrencies) and perform anonymously cyberattacks (through online anonymity and botnets).

(i) **Underground forums and markets:** Cybercriminals need to communicate together if they want to collaborate. This might explain the proliferation of online cybercriminal communities on darknet forums [69]. The rise of new and popular communication technologies is tied with the increasing problem of cybercrime [70]. This is because darknet or underground forums promote the trade of attack tools and services, making cyberattacks accessible for actors with low level of technical sophistication [69]. For a detailed examination of underground forums and markets we refer to [71].

(ii) **Cryptocurrency:** Cryptocurrency technically refers to a cryptographic string of numbers and alphabetic symbols, which together give a unique number and is considered a digital currency which

can be exchanged for real-life currencies [72]. It is a common way for cybercriminals to stay anonymous and conceal their money footprint [73]. The first darknet market to accept cryptocurrency was Silk Road in 2011. Although the business model of Silk Road was very successful, in 2013 the FBI shut it down. Nevertheless, cryptocurrency enabled to receive money anonymously. Nowadays most Law Enforcement agencies around the world have different methods to attribute crypto wallets to individuals. Therefore, cybercriminals often use mix services to hide money traces [72].

(iii) **Online anonymity:** The Internet community over the world is interested in anonymity. This led to the development of various anonymous networks. The most important are proxies, virtual private network (VPN) and The Onion Router (TOR) [74]. A VPN creates an encrypted connection over a less secure network, usually the internet, to send encrypted traffic [75]. The use of these technologies improves anonymity of internet users, both normal citizens but also criminals who want to hide their online activities [69, 76].

(iv) **Botnets:** Botnets are remotely controlled networks of computers, often with malicious aims [7]. The types and attack patterns of botnets constantly change, due to a large increase since 2016 in IoT devices which have enough processing power to be part of a botnet [77]. Botnets are most commonly used for DDoS attacks, but the infrastructure has also been used to spread phishing and malware [78], like for example the Emotet botnet.

Altogether, these developments led to the rise of:

(a) **Cybercrime-as-a-Service (CaaS):** Cybercrime-as-a-service is the phenomena that cybercriminals not only perform attacks themselves, but also buy or sell the tools and knowledge to other criminals to perform attacks [79]. Most criminal groups have become highly specialized in specific tools and methods to perform a specific part of an attack [80]. According to [81], CaaS leads to commoditization, specialization and cooperation of cybercriminals. Consequently, we can deduct that cybercrime-as-a-service leads to more interdependence between different cybercrimes, because criminals conducting different types of crime can work together to maximize profit.

(b) **Capabilities and resources:** Offenders can expand capabilities by learning from others through darknet forums. The required capabilities are an important distinction between cybercrimes like DDoS, phishing and ransomware. Ransomware is highly technical, phishing is medium difficult (also depending on web-based or email based phishing) and DDoS attacks are less technical [82]. This means that a non-technical actor could not use ransomware for a coordinated attack. One way to circumvent this problem is to buy tools and services from more technical actors, the phenomena CaaS. Nevertheless, not everything can be bought. For example, some actors who sell ransomware do not want to sell to newbies, because they might screw up and therefore get attention of Law Enforcement [42, 56].

(c) **Democratization of cybercrime:** The dissemination of cybercrime has been noted with respect to offenders as well as victims. Several authors noted that the step towards online offending has become easier over time, during the past decades. One does not need to be technically skilled, but with CaaS everyone can buy a phishing kit [81, 6] and start a phishing campaign or buy a DDoS attack and attack one's school [83]. The commoditization of attacks has led to a democratization of offending, according to [84, 85, 86]. A similar development is found with regard to victimisation. One of the consistent findings in traditional crime is that victims tend to be young and male, have a low educational level and are usually relatively poor [87, 88, 89] because it is strongly related to location and going out [90, 91, 92]. With the digitalization of society, however, offending and

victimization of cybercrime become much less related to location or being outdoors. Victims of online crime are both males and female, and for some crimes (online banking fraud, identity theft) of all ages or relatively old [84]. In summation, offenders as well as victims of online crime tend to be more than before a random – or 'normal' - selection of society.

These developments either directly or indirectly influence the costs and benefits of coordinated attacks. Therefore, it also influences an attacker's decision to perform a coordinated attack. Based on the information gathered in this paper we propose COORDINATE, a model to evaluate the costs and benefits of coordination for cybercriminals.

4.2 COORDINATE

From the empirical observations of coordination of DDoS, phishing, ransomware described in Section 3 and the evolution of the cybercrime ecosystem we hypothesise four types of coordination based on the costs and benefits of coordination for cybercriminals:

(i) **Direct collaboration:** One or multiple actors coordinate different attacks before performing the attacks. An example is when a ransomware group uses DDoS attacks to put pressure on a victim if he is not paying the ransom during a ransomware attack [9, 54, 53].

(ii) **Indirect collaboration:** One or multiple entities perform an attack and sell the end-product of that attack to other entities. For example: credentials gained from a phishing attack are sold to a ransomware group, who use the credentials to gain access to a system or network and install their ransomware [42, 49, 46].

(iii) **Opportunistic coordination:** One or multiple actors perform an attack. Subsequently, this becomes known to another actor. Subsequently, this actor uses this knowledge to enforce their own attack. For example: the media reports that a company is victim of a ransomware attack. A phishing group using this information as a context in their phishing email, sending them to the victim [2].

(iv) **Random coordination:** It might be that one or multiple offenders coordinate attack at random, and do not know their attack collides in some way with another attack. Then the attack looks like it is coordinated from a victim's perspective, although the offenders do not know this. A example is a bank who faces both phishing emails and DDoS attacks from two different entities, who do not know from each other an attack occurred [15]. Random coordination is outside the scope of the proposed model.

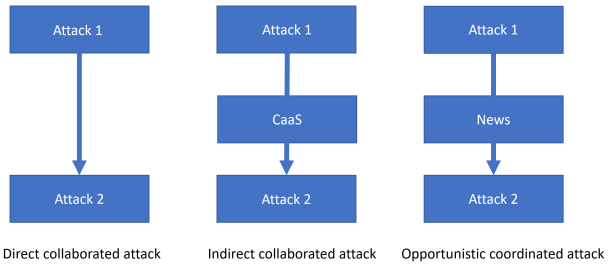

Figure 4: The different coordination types examined in this study.

The three relevant types of coordination are depicted in Figure 4. Note that it seems that one attack happens after the other, but this is not necessarily what is happening. For example, a DDoS attack could be a smokescreen for installing ransomware at the same time [57, 56]. Nevertheless, the coordination types are applicable to both sequential and parallel coordinated attacks. Here we define a sequential attack as two attacks with no overlap in time and a parallel attack as two attacks with overlap in time.

The various types of coordination lead to different ways of decision-making by an offender compared to no coordination in attack. The literature we found in Section 2 mostly focuses on how coordinated attacks could be performed, but not why the attacker would be motivated to do so. From a Rational Choice Perspective [93, 94], financially motivated cybercriminals try to maximize profits while minimizing costs and risks. Based on the use cases and developments presented in the previous sections, we hypothesize the following model, which we call COORDINATE: the CybercrimecOORDINATion modEl.

4.2.1 Benefits of coordination for cybercriminals

Performing a coordinated attack compared to a single attack leads to certain benefits. Based on Rational Choice Model of Crime [94], we argue that these benefits need to either increase profit, and/or decrease costs, risks and effort.

(i) **Profitability:** More profit per attack. Every successful attack will generate more profit. It can generate extra profit in two ways. 1) Larger companies or public organizations can be more successfully attacked. Therefore more ransom could be asked during a ransomware attack, or more money could be obtained with phishing or DDoS [95, 96]. 2) Every attack can generate revenue. For example, in a ransomware attack the attackers might gain the ransom, but also selling obtained credentials might directly provide in extra profits [81, 51]. Higher profit per attack could be most important in direct collaborated attacks, where offenders consciously collaborate, perhaps to go after a 'big fish'. It seems least applicable to opportunistic coordination, because they do not really apply specific targeting [97, 44].

(ii) **Success rate:** Higher probability of success per attack. By putting additional pressure on the victim during a ransomware attack or providing credible context in a phishing email, victims might be more willing to pay ransom or click on the link in the phishing email [9]. Sometimes the attack enables another attack, which means the probability goes from zero per cent (not possible) to a probability higher than zero per cent by coordinating the two attacks.

(iii) **Diffusion of responsibilities:** Coordination leads to diffusion of responsibilities: by performing a small part of the attack, the offender might feel less responsible for the attack [1]. Therefore moral costs are reduced: the feeling of doing something wrong might be less during a coordinated attack. This seems most applicable to indirect collaboration, where the offender selling their services or products do not necessarily know what the other offender is doing with the bought services or products. Diffusion of responsibilities may occur less often with direct collaboration, where an actor is in charge of the entire attack. Decreased moral costs could also occur with opportunistic coordination, since the offender of the second attack does not feel responsible for the first attack.

(iv) **Outsourcing:** Outsourcing the most risky or difficult parts of attack. In coordinated attacks, offenders could decide to perform the parts of an attack which have least risk of being detected or chased by Law Enforcement [81]. For example: they steal credentials or develop ransomware, but someone else deploy the ransomware [42, 47]. Law Enforcement tends to investigate the criminals behind the attack, and not the facilitators and enablers [98, 82]. Therefore, these have less risk of being caught and convicted. Advantages of outsourcing do not occur with direct collaboration,

since the offenders have to perform all the aspects of the attack themselves. It most probably happens with indirect collaboration, since many offenders offering their products or services actually offer tools or services to support an attack, but not perform the attack themselves. Finally, opportunistic offenders might only try attacks were they do the less risky attack. For example: they might execute phishing after a ransomware attack. In general, ransomware attacks often attracts more attention than phishing from Law Enforcement, because impact and severity is often higher. So by phishing after the ransomware, they might receive less attention from Law Enforcement compared to a single phishing attack.

(v) **Shielding:** Repeatedly performing a small part of an attack-type might lead to specialisation [81, 6]. Specialization might lead to better shielding techniques. This does not seem likely for direct collaborated coordinated attacks, because they perform the entire attack chain themselves. On the contrary, better shielding might drive indirect collaboration, where offenders on darknet forums are highly specialised and therefore might have more knowledge how to shield themselves. Likewise, in opportunistic coordinated attacks actors also can not perform the entire attack themselves, and therefore have better shielding compared to actors who are responsible for the entire attack, as in direct collaborated coordinated attacks.

Table 3: Overview proposed hypotheses of relationships between different costs and benefits in COORDINATE. ++ is a positive relationships, + is a small positive relationship, +/− no relationship, − is a small negative relationship, and −− is a negative relationship.

		Direct Collaboration	**Indirect Collaboration**	**Opportunistic Coordination**
Benefits	More profit	++	+	+/−
	Higher probability success	++	++	++
	Decrease moral costs	+/−	++	+
	Outsource most risky parts	+/−	++	+
	Better shielding	−−	++	+
Costs	Transaction costs	++	+	+/−
	Timing	+/−	+	++
	Extra effort	++	−	−−
	Financial costs	+	++	+/−
	Traces	++	+	+/−

4.2.2 Costs of coordination for cybercriminals

Coordinated attacks do not only have advantages, there are also costs:

(i) **Transaction costs**. If the coordinated attack is the result of a collaboration or cooperation of different actors, than this cooperation contains transaction costs [6, 99]. From Transaction Cost Economics these costs contain costs of working together, sharing profit, not knowing whether you could trust the other party, etc. [100, 6]. Since direct collaboration consists of the most intensive form of collaboration of all three, it follows that this would have the highest transaction cost, followed by indirect collaboration. Opportunistic coordination does not entail collaboration and therefore no transaction costs.

(ii) **Timing**. For some coordinated attacks timing is important. For example, when phishing for credentials to gain access to a network to install ransomware, the credentials might be invalid after a certain amount of time. Therefore the initial access broker can not wait too long for selling or using the credentials. Timing might be most important for opportunistic coordinated attacks, where they have to react to a another attack in time [15]. For direct collaboration timing might also be important between attacks, but they can decide themselves when the different attacks will be performed. So they are more in control over timing than opportunistic actors. Finally, products and services sold online are probably less time-sensitive than the other two, because it takes time for a vendor to find a buyer. So if timing was important, he would probably be not able to sell it through darknet forums.

(iii) **Extra effort**. Time and energy are required to perform a second attack if done by the same actor. Time spent on the second attack could not be used to do another separate attack, which would have also gained money. This is most important for coordination as a result of direct collaboration, since attackers have to coordinate all the attacks and make sure they have all capacities and resources to perform the attack. For example, if they try to find their own exploits, there is the risk of not finding any. Therefore, it is easier to perform a coordinated attack with products and services bought on darknet forums, and therefore effort should be less for a coordinated attack than uncoordinated attack. This could even more so for opportunistic attacks, they do not need to put any effort in the first attack. So attackers probably do not need to make more effort than if they would perform an uncoordinated attack.

(iv) **Financial costs**. Resources or capabilities needs to be bought, also, if one develops one's own software, than this also directly costs money. These costs are highest for goods and services bought on the darknet market, so indirect collaboration. Financial costs seems to be less so for direct collaboration, since attackers only need to buy resources and capabilities they do not have themselves. However, buying resources should be less expensive then end-products. Opportunistic actors do not have to pay anything to perform their coordinated attack, they just react to another attack.

(v) **Traces**. Performing more attacks will lead to more possible traces during an investigation of Law Enforcement. Therefore, performing coordinated attacks could increase the probability of getting caught. This seems most applicable to direct collaboration, since the same group of actors perform the different attacks, and therefore all attacks could be linked back to the group. This seems less applicable for indirect collaboration, because the attacks of criminals are only linked by a purchase over darknet. Linking attacks through darknet markets might be harder than a group with the same modus operandi. Since opportunistic coordinated attack do not have a link with the actors of the first attack, there are no extra traces compared to a single attack.

The hypotheses discussed above are summarised in Table 3.We believe these hypotheses need to be tested in further empirical research on coordination of cybercrime.

5 CONCLUSIONS

Although coordinated attacks have been described cybersecurity companies and blogs, to our knowledge no scientific research systematically studied coordinated cybercrimes. This paper set out to identify various ways attacks can be coordinated, describe recent developments w.r.t. coordination/cooperation concepts in cybercrime literature and provide a model of understanding the decision to coordinate attacks or not.

Our first research question: What is the current state of literature on the coordination and coordination of cybercrimes? We addressed this question by analysing the bibliometric mapping of academic literature, we found a cluster of studies which focuses on coordinated cyberattacks from the attackers perspective. They mostly focus on how these crimes can be coordinated, but not on the incentives for the attacker to do so. Therefore, our second research question was: What are the costs and benefits for an offender to decide to perform a coordinated attack or not? We addressed this question by introducing a case study of coordinating DDoS, phishing and ransomware. From the case study, specific vantage points for coordination were identified. Furthermore, through describing the recent developments in the cybercrime ecosystem, we explained why coordination becomes more feasible for attackers than it did previously. Finally, we deduced a hypothetical model we named the Cybercrime Coordination Model, COORDINATE. From this model we made testable predictions about the importance of certain costs and benefits towards the different types of coordinated attacks.

The results of this study indicate that coordinated attacks result in more harm and are, consequently, more dangerous. We showed that one can already observe attack coordination. If our model is correct, coordinated attacks will be produce more rewards for offenders at lower costs and therefore will occur more often in the future. We are therefore in danger of observing a dynamic system where one crime will lay-out opportunities for new crime that may lead to more and more online crime.

This study was limited by the absence of empirical data on coordinated cybercrimes in order to investigate the severity of such attack events. Despite its exploratory nature, this study offers some insight into the importance of coordinated cybercrimes. We hope this study will be a stepping-stone for other researchers to conduct empirical research on coordinated cybercrimes.

Acknowledgments

We would like to extend our sincere gratitude to the Dutch Police. In particular, we would like to thank Anne Jan Oosterheert, Cees van Tent, Rob Rulkens and Theo van der Plas for making the project possible. Furthermore, we like to thank the cybercrime unit East Netherlands and the Ransomware Taskforce for their expertise. Please note that the views expressed in this work are ours alone and do not necessarily reflect those of the Dutch Police.

References

[1] C.G.J. Putman and L.J.M. Nieuwenhuis. Business model of a botnet. In *Proc. of the 26th IEEE Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), Valladolid, Spain*, pages 441–445. IEEE, 2018.

[2] Security. Universiteit maastricht werd besmet via phishingmail en verouderde software. `https://www.security.nl/posting/642452/Universiteit+Maastricht+werd+besmet+via+phishingmail+en+verouderde+software`, 2020. Last checked on Jul 21, 2021.

[3] Lifars.com. Gangs launch ddos attacks to push victims into paying ransom. `https://lifars.com/2020/11/gangs-launch-ddos-attacks-to-push-victims-into-paying-ransom/`, 2020. Last checked on Jul 21, 2021.

[4] V. Yegneswaran, P. Barford, and J. Ullrich. Internet intrusions: Global characteristics and prevalence. *ACM SIGMETRICS Performance Evaluation Review*, 31(1):138–147, 2003.

[5] H.S. Lallie, K. Debattista, and J. Bal. A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, 35:100219, 2020.

[6] R. Van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C.H. Ganan, B. Klievink, N. Christin, and M. Van Eeten. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *Proc. of the 27th USENIX Security Symposium (USENIX), Baltimore, USA*, pages 1009–1026, 2018.

[7] Z. Bederna and T. Szádeczky. Effects of botnets–a human-organisational approach. *Security and Defence Quarterly*, 2021.

[8] E. R. Leukfeldt, E.R. Kleemans, and W.P. Stol. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, 57(3):704–722, 2017.

[9] Cyble. Uncensored interview with revil sodinokibi ransomware operators. https://blog.cyble.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/, 2021. Last checked on Jul 22, 2021.

[10] S. Shead. Symantec data stealing hackers use ddos to distract from attacks. https://www.zdnet.com/article/symantec-data-stealing-hackers-use-ddos-to-distract-from-attacks/, 2012. Last checked on Jul 25, 2021.

[11] Kaspersky. Research reveals hacker tactics: cybercriminals use ddos as smokescreen for other attacks on business. https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-busines 2016. Last checked on Jul 25, 2021.

[12] Group-IB. Silence moving into the darkside. https://www.group-ib.com/resources/threat-research/silence$_$moving-into-the-darkside.pdf, 2018. Last checked on Apr 25, 2021.

[13] D.E. O'Leary. What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis. *Journal of Information Systems*, 33(3):285–307, 2019.

[14] H. Oz, A. Aris, A. Levi, and A.S. Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *arXiv*, 2021.

[15] M. Junger, A. Abhishta, and L.J.M. Nieuwenhuis. Crime chain: het verband tussen ddos-aanvallen en phishing. 2021.

[16] P. Brereton, B.A. Kitchenham, D. Budgen, M. Turner, and M. Khalil. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software*, 80(4):571–583, 2007.

[17] D.N. Effendi, W. Anggraini, A. Jatmiko, H. Rahmayanti, I.Z. Ichsan, and M. Rahman. Bibliometric analysis of scientific literacy using vos viewer: Analysis of science education. 1796(1):012096, 2021.

[18] L.M. Mathews, A. Joshi, and T. Finin. Detecting botnets using a collaborative situational-aware idps. In *Proc. of the 2nd IEEE Second International Conference on Information Systems Security and Privacy (ICISSP), Rome, Italy*, 2016.

[19] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer. Hostage: a mobile honeypot for collaborative defense. In *Proc. of the 7th International Conference on Security of Information and Networks (SINCONF), Glasgow, UK*, pages 330–333, 2014.

[20] A. Petrillo, A. Pescape, and S. Santini. A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE transactions on cybernetics*, 51(3):1134–1149, 2020.

[21] P. Wang, X. Wu, and X. He. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. *Transportation Research Part C: Emerging Technologies*, 115:102625, 2020.

[22] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry. A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, 5(3):1183–1195, 2014.

[23] A. Attiah, M. Chatterjee, and C.C. Zou. A game theoretic approach to model cyber attack and defense strategies. In *Proc. of the IEEE International Conference on Communications (ICC), Kansas City, USA*, pages 1–7. IEEE, 2018.

[24] T. Grant, I. Burke, and R. Van Heerden. Comparing models of offensive cyber operations. *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security*, 2:35, 2015.

[25] F. Alserhani, M. Akhlaq, I.U. Awan, and A.J. Cullen. Detection of coordinated attacks using alert correlation model. In *Proc. of the IEEE International Conference on Progress in Informatics and Computing (PIC), Shanghai, China*, volume 1, pages 542–546. IEEE, 2010.

[26] S. Xu. Collaborative attack vs. collaborative defense. In *Proc. of the 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing (COLLABORATECOM), Orlando,*

USA, pages 217–228. Springer, 2008.

[27] H. He, S. Huang, Y. Liu, and T. Zhang. A tri-level optimization model for power grid defense with the consideration of post-allocated dgs against coordinated cyber-physical attacks. *International Journal of Electrical Power & Energy Systems*, 130:106903, 2021.

[28] H. Wang, X. Wen, S. Huang, B. Zhou, Q. Wu, and N. Liu. Generalized attack separation scheme in cyber physical smart grid based on robust interval state estimation. *International Journal of Electrical Power & Energy Systems*, 129:106741, 2021.

[29] J. C. J. Santanna. *DDoS-as-a-Service: investigating booter websites*. University of Twente, 2017.

[30] Debbie Walkowski. What is a distributed denial of service attack. `https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-`, 2019. Last checked on Sep 12, 2021.

[31] R. Vishwakarma and A.K. Jain. A survey of ddos attacking techniques and defence mechanisms in the iot network. *Telecommunication Systems*, 73(1):3–25, 2020.

[32] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[33] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13(12):1550147717741463, 2017.

[34] A. Abhishta. *The blind man and the elephant: Measuring economic impacts of ddos attacks*. University of Twente, 2019.

[35] M. A. Ivanov, B.V. Kliuchnikova, I.V. Chugunkov, and A.M. Plaksina. Phishing attacks and protection against them. In *Proc. of the 1st IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Moscow, Russia*, pages 425–428. IEEE, 2021.

[36] E.E.H. Lastdrager. *From fishing to phishing*. University of Twente, 2018.

[37] David Warburton. 2020 phishing and fraud report. `https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report`, 2020. Last checked on Sep 12, 2021.

[38] A. Darwish, A. El Zarka, and F. Aloul. Towards understanding phishing victims' profile. In *Proc. of the IEEE International Conference on Computer Systems and Industrial Informatics (ICCSII), Sharjah, UAE*, pages 1–5. IEEE, 2012.

[39] B.B. Gupta, A. Tewari, A.K. Jain, and D.P. Agrawal. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12):3629–3654, 2017.

[40] R. Al Halaseh and J. Alqatawna. Analyzing cybercrimes strategies: The case of phishing attack. In *Proc. of the IEEE Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan*, pages 82–88. IEEE, 2016.

[41] A. Oest, P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupé, and G. Ahn. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *Proc. of the 29th USENIX Security Symposium (USENIX), Santa Clara, USA*, pages 361–377, 2020.

[42] N. Hassan. *Ransomware Revealed*. Springer, 2019.

[43] R. Sobers. Data breach investigations report. `https://www.varonis.com/blog/ransomware-statistics-2021/`, 2021. Last checked on Jul 19, 2021.

[44] L.Y. Connolly, D.S. Wall, M. Lang, and B. Oddson. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, 6(1):1–18, 2020.

[45] M. Humayun, N.Z. Jhanjhi A. Alsayat, and V. Ponnusamy. Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, 22(1):105–117, 2021.

[46] M. Hijji and G. Alam. A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: Challenges and prospective solutions. *IEEE Access*, 9:7152–7169, 2021.

[47] L.Y. Connolly, M. Lang, P. Taylor, and P.J. Corner. The evolving threat of ransomware: From extortion to blackmail. 2021.

[48] M. Loman. How ransomware attacks. *Sophos*, 2019.

[49] A. Zimba and M. Chishimba. On the economic impact of crypto-ransomware attacks: the state of the art on enterprise systems. *European Journal for Security Research*, 4(1):3–31, 2019.

[50] Z. Li and Q. Liao. Game theory of data-selling ransomware. *Journal of Cyber Security and Mobility*, pages 65–96, 2021.

[51] C. Simoiu, A. Zand, K. Thomas, and E. Bursztein. Who is targeted by email-based phishing and malware? measuring factors that differentiate risk. In *Proc. of the 20th ACM Internet Measurement Conference (IMC), Virtual*, pages 567–576, 2020.

[52] Borislav Tonev. Cyber attack guide ddos attacks. https://www.scalahosting.com/blog/cyber-attack-guide-ddos-attacks/, 2021. Last checked on Jul 22, 2021.

[53] Sean Newman. How ransomware is teaming up with ddos. https://www.infosecurity-magazine.com/opinions/ransomware-teaming-ddos/, 2021. Last checked on Jul 21, 2021.

[54] Lawrence Abrams. Another ransomware now uses ddos attacks to force victims to pay. https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/, 2021. Last checked on Aug 19, 2021.

[55] Victoria Kivilevich. Ransomware gangs are starting to look like oceans 11. https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/, 2021. Last checked on Jul 22, 2021.

[56] A. Liska and T. Gallo. *Ransomware: Defending against digital extortion*. O'Reilly Media, 2016.

[57] Corero. The links between ransomware and ddos attacks. https://www.corero.com/blog/the-links-between-ransom-ransomware-and-ddos-attacks/, 2021. Last checked on Jul 22, 2021.

[58] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainuddin Mohd Shaid. A 0-day aware crypto-ransomware early behavioral detection framework. In *Proc. of the 2nd International Conference of Reliable Information and Communication Technology (IRICT), Johor Bahru, Malaysia*, pages 758–766. Springer, 2017.

[59] KnowBe4. Whos behind this massive wave of ddos and phishing attacks targeting dutch banks. https://blog.knowbe4.com/whos-behind-this-massive-wave-of-ddos-and-phishing-attacks-targeting-dutch-banks, 2021. Last checked on Jul 25, 2021.

[60] M. Kotadia. Ddos makes a phishing e-mail look real. https://www.zdnet.com/article/ddos-makes-a-phishing-e-mail-look-real/, 2006. Last checked on Jul 25, 2021.

[61] F. Hassandoust, H. Singh, and J. Williams. The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, 24, 2020.

[62] S. Mansfield-Devine. The evolution of ddos. *Computer Fraud & Security*, 2014(10):15–20, 2014.

[63] M. Sauter. "loic will tear us apart" the impact of tool design and media portrayals in the success of activist ddos attacks. *American Behavioral Scientist*, 57(7):983–1007, 2013.

[64] Y. Kwak, S. Lee, A. Damiano, and A. Vishwanath. Why do users not report spear phishing emails? *Telematics and Informatics*, 48:101343, 2020.

[65] J.W. Bullee, L. Montoya, M. Junger, and P. Hartel. Spear phishing in organisations explained. *Information & Computer Security*, 2017.

[66] A. Oest, Y. Safei, A. Doupé, G. Ahn, B. Wardman, and G. Warner. Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In *Proc. of the 13th APWG Symposium on Electronic Crime Research (eCrime), San Diego, USA*, pages 1–12. IEEE, 2018.

[67] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, and H. Liu. Click trajectories: End-to-end analysis of the spam value chain. In *Proc. of the 32nd IEEE Symposium on Security and Privacy (SP), Oakland, USA*, pages 431–446. IEEE, 2011.

[68] S. Broadhead. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, 34(6):1180–1196, 2018.

[69] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery. Characterizing eve: Analysing cybercrime actors in a large underground forum. In *Proc. of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), Heraklion, Greece*, pages 207–227. Springer, 2018.

[70] A. Sutanrikulu, S. Czajkowska, and J. Grossklags. Analysis of darknet market activity as a country-specific, socio-economic and technological phenomenon. In *Proc. of the IEEE APWG Symposium on Electronic Crime Research (eCrime), Virtual*, pages 1–10. IEEE, 2020.

[71] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian. Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *Proc. of the 14th IEEE Conference on Intelligence and Security Informatics (ISI), San Antonio, USA*, pages 7–12. IEEE, 2016.

[72] E. Reddy and A. Minnaar. Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3):71–92, 2018.

[73] L.Y. Connolly and D.S. Wall. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, 87:101568, 2019.

[74] E. Ramadhani. Anonymity communication vpn and tor: a comparative study. In *Journal of Physics: Conference Series*, volume 983, page 012060. IOP Publishing, 2018.

[75] A. Pavlicek and F. Sudzina. Use of virtual private networks (vpn) and proxy servers: Impact of personality and demographics. In *Proc. of the 13th International Conference on Digital Information Management (ICDIM), Berlin, Germany*, pages 108–111. IEEE, 2018.

[76] P.H. Meland, Y.F.F. Bayoumy, and G. Sindre. The ransomware-as-a-service economy within the darknet. *Computers & Security*, 92:101762, 2020.

[77] S.N.T. Vu, M. Stege, P.I. El-Habr, J. Bang, and N. Dragoni. A survey on botnets: Incentives, evolution, detection and current trends. *Future Internet*, 13(8):198, 2021.

[78] T.T. Sigurdardottir and S. Neubauer. Emotet from a banking trojan to one of the most advanced botnets. `https://www.cyren.com/blog/articles/emotet-from-a-banking-trojan-to-one-of-the-most-advanced-botnets`, 2019. Last checked on Jul 22, 2021.

[79] D. Manky. Cybercrime as a service: a very modern business. *Computer Fraud & Security*, 2013(6):9–13, 2013.

[80] T.S. Hyslip. Cybercrime-as-a-service operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pages 815–846, 2020.

[81] K. Huang, M. Siegel, and S. Madnick. Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys*, 51(4):1–36, 2018.

[82] Verizon. Data breach investigations report. `https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf`, 2020. Last checked on Jul 19, 2021.

[83] A. Abhishta, M. Junger, R. Joosten, L.J.M. Nieuwenhuis, and J.M. Lambert. Victim routine influences the number of ddos attacks: Evidence from dutch educational network. In *Proc. of the 40th IEEE Security and Privacy Workshops (SPW), San Fransisco, USA*, pages 242–247. IEEE, 2019.

[84] M. Junger, L. Montoya, P. Hartel, and M. Heydari. Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe. In *Proc. of the IEEE International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), London, UK*, pages 1–8. IEEE, 2017.

[85] A. Noroozian. *Evaluating Hosting Provider Security Through Abuse Data and the Creation of Metrics*. TU Delft, 2020.

[86] J. Jansen, M. Junger, L. Montoya, P. Hartel, and W.P. Stol. Offenders in a digitized society. *Cybercrime and the Police*, pages 45–59, 2013.

[87] J. Bunch, J. Clay-Warner, and M.K. Lei. Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency*, 61(9):1181–1205, 2015.

[88] D.C. Gottfredson. An empirical test of school-based environmental and individual interventions to reduce the risk of delinquent behavior. *Criminology*, 24(4):705–731, 1986.

[89] J.L. Lauritsen, R.J. Sampson, and J.H. Laub. The link between offending and victimization among adolescents. *Criminology*, 29(2):265–292, 1991.

[90] J.L. Lauritsen, J.H. Laub, and R.J. Sampson. Conventional and delinquent activities: Implications for the

prevention of violent victimization among adolescents. *Violence and victims*, 7(2):91–108, 1992.

[91] E.E. Mustaine and R. Tewksbury. Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, 36(4):829–858, 1998.

[92] A. Tseloni, K. Wittebrood, G. Farrell, and K. Pease. Burglary victimization in england and wales, the united states and the netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, 44(1):66–91, 2004.

[93] L.E. Cohen and M. Felson. Social change and crime rate trends: A routine activity approach. *American sociological review*, pages 588–608, 1979.

[94] D.B. Cornish and R.V. Clarke. Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4):933–948, 1987.

[95] E. R. Ritenour. Hacking and ransomware: challenges for institutions both large and small. *American Journal of Roentgenology*, 214(4):736–737, 2020.

[96] M. Hijink. Onderhandelen over gijzelsoftware: 'we hadden toch 10 miljoen afgesproken?'. *NRC*, 2021.

[97] L.Y. Connolly and D. Wall. Hackers are making personalised ransomware to target the most profitable and vulnerable. *The Conversation*, 15, 2019.

[98] N. Popper. Ransomware attacks grow, crippling cities and businesses. *The New York Times*, 2020.

[99] G. Zhou, J. Zhuge, Y. Fan, K. Du, and S. Lu. A market in dream: the rapid development of anonymous cybercrime. *Mobile Networks and Applications*, 25(1):259–270, 2020.

[100] O.E. Williamson. Transaction cost economics and organization theory. *Industrial and Corporate Change*, 2(2):107–156, 1993.

Author Biography

Tom Meurs received the B.S. degree in Methodological Psychology in 2016 and B.S. and M.S. degrees in Econometrics from the University of Amsterdam in 2017 and 2018. He is currently a Ph.D. candidate at the University of Twente. The PhD project is funded by the Dutch Police. His research interests include ransomware, coordination of cybercrimes, Initial Access Brokers and communication between cybercriminals.

Marianne Junger received the Ph.D. degree in law from the Free University of Amsterdam, Amsterdam, the Netherlands, in 1990. She is the Emeritus Professor of Cyber Security and Business Continuity with the University of Twente, Enschede, the Netherlands. Her research investigates the human factors of fraud and cybercrime. More specifically, she investigates online victimization, disclosure, and privacy issues. She founded the Crime Science journal together with Pieter Hartel and was an Associate Editor for 6 years. Her research was sponsored by, among others, the Dutch Police, NWO, ZonMw (for health research), and the European Union.

Abhishta Abhishta is an assistant professor at the High-tech Business and Entrepreneurship department at University of Twente. His research focuses on empirically measuring the economic/financial impact of cyber attacks. To do so, he devises/adapts data-driven economic impact assessment techniques. He looks to help organisations make well-measured investments in security. His doctoral research was funded under NWO project D3 – Distributed Denial-of-Service Defense: protecting schools and other public organizations. His current research is supported by two NWO grants,

one aimed at cloud security (MASCOT) and the other at building a first prototype of the Responsible Internet (CATRIN). He serves on the program committee of ACM/IEEE/IFIP conferences aimed at network measurements and responsible internet (TMA, PAM, TAURIN).

Erik Tews is a security researcher who spent most of his academic life at Technische Universität Darmstadt, Germany. Previously he was working for the University of Birmingham, UK and since 2017, he is at the University of Twente. He is currently interested in the Internet of Things, privacy preserving technologies, the World Wide Web Applied Cryptanalysis including side channel attacks, railway signalling systems, security of critical infrastructures and security of wireless protocols.

Emma Ratia is a Finnish-Dutch cultural anthropologist, all-round researcher and analist with an interest on the social side of cybercrime. In her work she combines social scientific insights with day-to-day operational work on cybercrime within the Dutch National Police.