Csaba Krasznay

Case Study: The NotPetya Campaign

Introduction

The range of malicious acts affecting cyberspace is endless, but there are events that provide a red line and a point of reference for researchers. The attack on Estonia in 2007, the deployment of the Stuxnet malicious code, the leak of information by Edward Snowden were all such events when we had to re-evaluate our views on cyberspace. From the perspective of the present study, the NotPetya malicious code campaign is a turning point that explains the importance of international law and international relations in connection to cyber events. This incident has highlighted some critical points on the field of external relations, which showed in practice that the creation of the Tallinn Manual or the proposal for a Digital Geneva Convention was necessary because of the practice of some countries in interpreting international norms freely.

The Technical Perspective

According to a summary in the *Wired* magazine, the NotPetya campaign started on the afternoon of 27 June 2017, in the last working hours of the working day before the celebration of the Ukrainian Constitution. The date of the first infections was food for thought, as choosing a prominent holiday of the Republic of Ukraine as the beginning of the attack was a signal message. Meanwhile, at that moment it was still probable that the time was also chosen according to a plan based on the fact that the majority of IT operators would be on leave, so the defence would work with lower resources. Although the malware appeared soon in other countries, most of the infected machines were reported from Ukraine, so it is suspected that the target was Ukraine as a state and not some companies were on the crosshairs. In other countries, including Germany, France, Italy, Poland and the United States, there were only collateral damages. This theory is

https://doi.org/10.36250/01039_05

further reinforced by the fact that an explosive device hidden in a motor vehicle killed a member of the Special Forces in Kiev on the same day.[1]

The malicious code had the characteristics of a ransomware, encrypting the hard drive after infection, and asking for 300 USD in bitcoin in exchange for unlocking the machine. However, it soon became clear that the email address provided for the contact was not alive, so there was no chance of recovering the lost data. If the attack was financially motivated, as in the case of WannaCry a month before NotPetya, the attacker would have remained available and would have secured the return of the data in exchange for a ransom, as the victim only paid if there was a chance for the decryption as it was learnt from similar crimes. The characteristics of a ransomware in the early hours was also emphasised by the fact that the code showed similarities to the well-known Petya ransomware, but it was soon discovered that it was intentional camouflage, so the name NotPetya, or Non Petya, became widespread among cybersecurity experts.

In terms of mechanism of action, the malicious code infected the computer's master boot record, the hard disk segment responsible for loading the operating system, and began encrypting the file system after the machine was started. If that succeeded, it showed a typical ransomware message on the screen, indicating how much money it was asking for the decryption and how the communication was possible with the cybercriminals. Before making the machine unusable, it tried to spread to the network on which the infected machine was located. It used the EternalBlue vulnerability, and as it could be seen in case of WannaCry, it started to spread on the previously non-updated computers, meanwhile it collected the administrator password from the infected machine's memory, that also could give access to other networked machines.

The first infections were assumed to have come through a software update mechanism of the MEDoc application. This software is one of the officially approved tax return programs, so it runs on a significant part of Ukrainian companies. This program indicated that it needed to be updated, and then after the user allowed the patches to be installed, the infection began. There is no information on how they could influence the MEDoc update process. From remote hacking to direct, physical access to the update server, there are a number of possible solutions to consider. It seems certain that the attacker gained administrative privileges on one of MEDoc's servers, which allowed him to intervene in the

[1] Andy Greenberg: Petya Ransomware Epidemic May Be Spillover From Cyberwar. *Wired,* 28 June 2017.

update mechanism as well. According to an investigation by the cybersecurity company Talos, as early as 24 April 2017, an update was released to users that included a backdoor, so in principle, it allowed the attack to be carried out. Therefore, the attackers started preparing for the action months earlier. Against WannaCry, there was not any hidden code or so-called "kill switch", which would have enabled the rapid shutdown of the infection. The attacker's goal was clearly the largest, geographically most localised destruction.[2]

Eventually, thousands of Ukrainian companies were hit by the incident. The victims include certain critical Ukrainian infrastructures, including Ukrainian banks, the Kiev Borispol Airport, and energy companies such as Kyivenergo and Ukrenergo. But several foreign companies have also reported infections, such as the American medical company Merck, the Russian Rosnyeft and the Hungarian OTP Bank in Ukraine, whose ATMs displayed the images of the NotPetya infection for days. Most publicity was given to the devastation at A. P. Moller – Maersk. This company is the 558th largest conglomerate in the world according to the Forbes Global 2000 list of companies, one of the largest logistics companies in the world. The NotPetya infection reportedly made it impossible for the company to operate for two days. Loading of cargo ships worldwide had to be controlled manually, relying on paper and pencil instead of a computer. This was also reflected in the Danish company's revenue, with their quarterly report estimating that they suffered between $200 million and $300 million in damage from this two-day shutdown.[3]

International Law Perspective

The NotPetya malicious code is the first cyber incident that appears to be a coordinated attack on a sovereign state in peacetime, attacking its critical infrastructures, civilian facilities, causing additional damage to civilian companies operating in other countries as well. Its purpose was clearly destruction. Tools used by the malicious code were previously known, as neither the vulnerability exploited for network propagation nor the software that was used to access the credentials of privileged users caused a surprise to professionals. However, attack

[2] David Maynor et al.: The MeDoc Connection. *Talos Intelligence,* 05 July 2017.

[3] Maersk Press Room: *A. P. Moller – Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year.* 16 August 2017.

tactics were completely new, preceded by a thorough operational planning, as the MEDoc software chosen for distribution was unknown beyond Ukraine, only adequate intelligence could confirm that this propagation vector could be so effective in carrying out a geographically focused cyberattack. The psychological or social engineering twist in the attack should also be emphasised, which led the victims to believe that a version of MEDoc that would open a backdoor for malicious code should be installed. For decades, cybersecurity professionals have been aware that both end-users and IT operators need to use the latest version of software, so if a software update is available, it should be installed as soon as possible. Therefore, the attacker built the distribution on this foundation, believing that users would install anything that appears to be an update as soon as possible, without question, so attacking the update server and using it as a distribution point is a brilliant choice.

From the states' perspective, the right answer should be decided if there is a cybersecurity incident that looks like a cyberwarfare activity, in which an advanced cyber weapon was deployed in a country that has previously suffered such targeted attacks and it is used regularly as a weapons test site by another country. Can it be said that this incident is classified as an attack within the meaning of international law? Can they use the means of attribution, or name a country an attacker? On the other hand, the question is also whether international diplomacy is prepared to deal with the countermeasures of the named country by traditional diplomatic means after such a declaration? Finally, the question is also whether the named attacking country can be put under pressure as a result of which it will reduce or end its hostilities in cyberspace?

Schmitt and Biller examined how the incident relates to the requirements of international law a few weeks after the NotPetya attack. Their first remark was that the malicious code was not reported to have caused injury or death. The author of the present study adds that, although no direct deaths were reported for either NotPetya or WannaCry, it cannot be excluded that non-functioning electronic information systems in some healthcare facilities, especially in case of WannaCry, may have contributed indirectly to deaths in the U.K. healthcare system that could have been prevented if the patient had been provided with appropriate care in a timely manner. Schmitt and Biller link accountability to attribution, i.e. the main question is whether the attack was backed by a country's armed forces, intelligence agencies, or whether the instructions were given by a state actor in case of a non-state attacker. Assuming that this has happened, a breach of three state obligations can be presumed. These are

respect for sovereignty, the principle of non-interference and the prohibition of the use of force.

According to Schmitt and Biller, sovereignty was violated during the NotPetya attack because of two conditions. On the one hand, a violation of territorial integrity, which in cyberspace can be imagined as an attack causing physical damage or personal injury, possibly death. In a broad interpretation, if a cyber infrastructure becomes unavailable for an extended period of time, in the opinion of the authors, a violation of territorial integrity can also be formulated. Because NotPetya went beyond the effects of an average distributed denial of service attack, specifically involving the loss of key data and the need to deploy new machines instead of disrupted critical computer systems, this can be seen as damage to physical facilities. The other condition would be the disruption of core government activities, but this was not the case for NotPetya. Although the IT systems that enable financial institutions to operate are damaged, they do not support basic government functionality, so this condition for violating sovereignty did not exist.

Violations of the principle of non-interference are accompanied by coercive actions taken by one state against another in order to change its political, economic, social and cultural order and to influence foreign policy. Schmitt and Biller did not see evidence that the NotPetya malicious code was capable of achieving these purposes, given that its purpose was destruction and not influence. If the cyber weapon had indeed been a ransomware virus, which seemed at first glance, coercion would in principle have been possible since the essence of ransom is to extort some decision from the other party.

The principle of the use of force in peacetime means that a state engages in a violent activity that does not qualify as self-defence or collective defence without a UN mandate. Activities in the cyberspace typically have little impact on the physical environment, making it difficult to imagine an attack that reaches an unauthorised level of use of force. The long-term outage of a cyber infrastructure as computers or network devices become inaccessible due to a malicious code like NotPetya, however, could be classified as unauthorised use of force. According to the authors, economic destabilisation may also fall into this category. According to the Ukrainian Government, the cyberattack has reached this level, but international practice in mid-2017 has not yet provided a clear answer as to where the threshold is.

The authors' opinion is that international humanitarian law would be valid in this case if there were an international armed conflict between two states, namely

Ukraine and, suppose, Russia. The condition in that case is that one country occupies the territory of another country or supports a non-state group that engages in hostile activity against the other country. Given the support of the Crimean Peninsula and the uprisings in eastern Ukraine, the authors see a legitimate presumption of an armed conflict between the two states, therefore the use of NotPetya should also be examined under international humanitarian law, despite the fact that in the UN GGE there is no full agreement on this.[4] The classification of this malicious code should be examined in the light of the Tallinn Handbook, which states that the use of such cyber weapons is an attack even if it does not directly damage the cyber infrastructure, only has indirect effects. According to some experts, the inaccessibility of such infrastructure also belongs to that set.

NotPetya's targets included the Kiev Airport, the Chernobyl power plant, and the Ukrainian healthcare system. If it can be assumed that this was done in accordance with the attacker's intention and not due to the uncoordinated spread of the malicious code, this can be classified as an attack according to the authors. Although some of the disputed facilities could be classified as dual use, such as the airport, most elements of cyber infrastructure are clearly civilian, not serving military purposes, so the act could even fall into the category of a war crime. In addition, the impact of cyber weapons went beyond Ukraine, it also had an impact on third countries, so their neutrality was violated by the attacker.[5]

All of these are, of course, only the scientific thinking of researchers, as mentioning war crimes in case of a cyberattack can have serious diplomatic implications, if it is done by a politician in charge. As it can be read in the next chapter, states use moderate expressions, even if they have a strong diplomatic reaction. NotPetya, on the other hand, is special that in addition to researcher positions, there have been comments and then political resolutions that should be taken more seriously than theoretical reasoning. First, researchers from NATO's Center for Excellence in Cooperative Cyber Defense analysed the situation. The quoted Michael Schmitt also belongs to this scientific circle, but the analysis quoted earlier did not appear on the organisation's website, therefore the article by Blumbergs, Minárik, van der Meij and Lindström has already been published by the world press as NATO's position. Thus, special emphasis is placed on what Minárik said:

[4] Michael N. Schmitt – Liis Vihul: International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security,* 30 June 2017.

[5] Michael N. Schmitt – Jeffrey Biller: The NotPetya Cyber Operation as a Case Study of International Law. *EJIL:Talk!,* 11 June 2107.

"If the operation is related to an international armed conflict, it is subject to the legislation on armed conflict." Previously, NATO CCD COE commentaries had not visited the world press on such a delicate matter, so it could be perceived that NotPetya weighed significantly more than any other previous case.[6]

The States' Answer

Countries were not prepared for such a serious violation of international norms. The really big breakthrough came only in February 2018, when 7 countries, the United States, the United Kingdom, Denmark, Lithuania, Estonia, Canada and Australia, jointly condemned Russia for the NotPetya attack, which was officially supported by New Zealand, Norway, Latvia, Sweden and Finland. Never before have several countries used the means of attribution together, that is, they have pointed out the attacker in unison. Attribution is always a political decision that can be supported by technical or intelligence evidence, but without political will, they are not worth much. Tobias Feakin, Australia's Ambassador for Cyber Affairs, summed up excellently why this joint stand was an important step and what it means for the attackers:

> "What we're doing is maturing this approach in order that the consequences will be felt further in the future. So another key part of deterrence is signalling to another country, to provide clear, consistent, and credible messaging to adversaries that there will be repercussions for the behaviour that they're conducting."[7]

Depending on the attribution's certainty, there are several tools in the hand of nation states to give answer to a cyberattack. Moret and Pawlak give an example, how individual countries or EU institutions, member states in the EU Council or the EU in cooperation with international organisations can choose from the following answers:

- statements and demarches
- international agreements

[6] Bernhards Blumbergs et al.: NotPetya and WannaCry Call for a Joint Response from International Community. *NATO CCD COE,* 2017.

[7] Stilgherrian: Blaming Russia for NotPetya was Coordinated Diplomatic Action. *ZDNet,* 11 April 2018.

- capacity building
- strategic communication
- joint investigations
- statements by HR/VP
- EU demarches
- formal request for assistance
- Council conclusions
- political and cyber dialogues
- recalling diplomats
- sanctions
- solidarity clause
- countermeasures
- Mutual Defence Clause
- military response[8]

At the time of NotPetya only the United States implemented unilateral cyber sanctions. In 2015, President Barack Obama used this format against North Korea in response to the attack against Sony Pictures. Therefore, other countries have not had any tested and proven responses against devastating cyberattacks. Until 2017, most countries officially treated the threats in cyberspace as an internal defence question; however, they agreed that international norms and legislation are valid in the cyberspace as well. Attribution, diplomatic or even military responses were not part of the common diplomacy toolbox. Only the United States had enough power to publicly attribute another country, generally speaking Russia, Iran and North Korea in connection with cyberattacks. That is why NotPetya was a game changer. The U.S. Government attributed the NotPetya attack to Russia with the following statement from the Press Secretary of the White House:

> "In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences."[9]

[8] Erica Moret – Patryk Pawlak: The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? *EUISS,* July 2017.

[9] The White House: *Statement from the Press Secretary.* 15 February 2018.

The Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (DHS) together with the Federal Bureau of Investigation (FBI) even created a separate investigation and attribution stream to the Russian cyberattacks. It is called Grizzly Steppe. Both agencies analyse the tactics, techniques and procedures (TTPs as it is used in cybersecurity) of Russian state sponsored actors. Codename Grizzly Steppe was chosen right after the alleged intervention of Russian secret services in the 2016 Presidential Election. The list of cyberattacks was later enhanced with NotPetya and the cyber activity of the Russian Government targeting energy, other critical infrastructure sectors and network infrastructure devices.[10] DHS summarised such activities with the following sentences:

> "Russia's civilian and military intelligence services engaged in aggressive and sophisticated cyber-enabled operations targeting the U.S. government and its citizens. The U.S. Government refers to this activity as GRIZZLY STEPPE. These cyber operations included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, and theft of information from these organizations. This stolen information was later publicly released by third parties. In operations targeting other countries, including U.S. allies and partners, Russian intelligence services (RIS) have undertaken damaging or disruptive cyber-attacks, including on critical infrastructure—in some cases masquerading as third parties or hiding behind false online personas designed to cause the victim to misattribute the source of the attack."[11]

Such approach is not surprising from the United States. It uses a very straight diplomatic language against its main global competitors and especially in cyber cases, it always tries to clarify the boundaries of acceptable international norms. Until the 2015 meeting of President Barack Obama and President Xi Jinping when the two leaders agreed on major cybersecurity questions, U.S. officials mainly remembered about the unacceptable behaviour of China. Later on, the U.S. seemingly forgot China and turned to Russia. In 2020, the U.S. criticises China again, following its general foreign policy.

A similar approach can be seen in other countries. Close U.S. allies like the United Kingdom or Australia also had clear statements on NotPetya. On

[10] Cybersecurity and Infrastructure Security Agency: *Grizzly Steppe – Russian Malicious Cyber Activity.* 16 April 2018.

[11] Department of Homeland Security: *Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale.* 30 December 2016.

15 February 2018, U.K. Foreign Office Minister Lord Ahmad attributed this cyberattack to Russia highlighting that the U.K. and its allies will not tolerate malicious cyber activities.

> "The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017. The attack showed a continued disregard for Ukrainian sovereignty. Its reckless release disrupted organisations across Europe costing hundreds of millions of pounds. The Kremlin has positioned Russia in direct opposition to the West yet it doesn't have to be that way. We call upon Russia to be the responsible member of the international community it claims to be rather then secretly trying to undermine it. The United Kingdom is identifying, pursuing and responding to malicious cyber activity regardless of where it originates, imposing costs on those who would seek to do us harm. We are committed to strengthening coordinated international efforts to uphold a free, open, peaceful and secure cyberspace."[12]

The United Kingdom, part of the Five Eyes countries and closest ally of the U.S. is also very straight with Russia; unsurprisingly, Russia has many active operations on the island.

On the next day, 16 February 2018, Australian Minister for Law Enforcement and Cyber Security, Angus Taylor released the following statement:

> "Australian Government attribution of the 'NotPetya' cyber incident to Russia. The Australian Government has joined the governments of the United States and the United Kingdom in condemning Russia's use of the 'NotPetya' malware to attack critical infrastructure and businesses in June 2017. Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian Government has judged that Russian state sponsored actors were responsible for the incident. Computers were infected by a sophisticated piece of malware – or malicious software – that masqueraded as ransomware. 'NotPetya' interrupted the normal operation of banking, power, airports and metro services in Ukraine. While the brunt of the impact was felt in Ukraine, the malware spread globally, affecting a number of major international businesses causing hundreds of millions of dollars in damage. The Australian Government condemns Russia's behaviour, which posed grave risks to the global economy, to government operations and services, to businesses activity and the safety and welfare of individuals. The Australian Government is further strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace. The Government is committed to ensuring the Australian public sector, businesses and the community are prepared for evolving cyber threats."[13]

[12] Foreign and Commonwealth Office: *Foreign Office Minister Condemns Russia for NotPetya Attacks.* 15 February 2018.

[13] Parliament of Australia: *Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia.* 16 February 2016.

Australia is more exposed to Chinese cyberattacks, therefore it rarely deals with Russian originated attacks. We can treat this remark as a polite gesture for the United States.

Estonian Minister of Foreign Affairs, Sven Mikser reflects to the U.K. Government in his press release:

> "The NotPetya cyber-attack which targeted Ukraine's financial, energy and government sectors and undermined the sectors' resilience, demonstrated disrespect for Ukrainian sovereignty and caused significant economic losses in other countries too. It is very important for Estonia to maintain an open, stable and secure cyber space and for that, countries have to act responsibly and follow the rules of international cooperation and the norms of international law that apply in cyber space just like everywhere else."[14]

Estonia is the closest ally of the United States in the Baltic region and has the closest ties towards the U.S. in cybersecurity. They were also the first country that suffered a devastating cyberattack from Russia. Estonians are also pioneering in cyber diplomacy. It is not surprising that that full support was given for the attribution.

As we can see, those countries who officially attributed the cyberattack to Russia, draw up their views by the foreign ministers or ministers responsible for cybersecurity. Supporting nations of this diplomatic step also emphasised the role of Russia, but the announcements were made by lower ranked government officials. For example, in New Zealand, Director-General of the Government Communications Security Bureau (GCSB) Andrew Hampton released the statement.

> "While NotPetya masqueraded as a criminal ransomware campaign, its real purpose was to damage and disrupt systems […]. Its primary targets were Ukrainian financial, energy and government sectors. However, NotPetya's indiscriminate design caused it to spread around the world affecting these sectors world-wide. While there were no reports of NotPetya having a direct impact in New Zealand, it caused disruption to some organisations while they updated systems to protect themselves from it. This reinforces that New Zealand is not immune from this type of threat. In a globally connected world our relative geographic isolation offers no protection from cyber threats. We support the actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity."[15]

[14] Republic of Estonia: *Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine.* 15 February 2018.

[15] Government Communications Security Bureau: *New Zealand Joins International Condemnation of NotPetya Cyber-attack.* 16 February 2018.

New Zealand, like Australia is far from Russia and has much more problems in the cyberspace with China. As member of the Five Eyes countries, it supported the attribution, but we can assume that the government has not given high priority for this issue.

In case of Latvia, the public reaction was a short message on Twitter from the Ministry of Foreign Affairs: "#Latvia is deeply concerned about the findings of UK & US attribution of #NotPetya #Cyber_attacks and stands for responsible state behaviour in cyberspace." In case of a country with 27% of native Russians, even a tweet can be a strong support towards its NATO allies.

Deterrence in Cyberspace

NotPetya was the red line for Western countries that invoked not only diplomatic reactions as it was mentioned in the previous section, but after 2018, some countries, especially the United States have publicly introduced some retaliatory actions against Russia. This is not surprising as according to the traditional deterrence theory, three elements should be present to stop a rogue activity: attribution, credible signalling and deterrence strategies. Taddeo explains that as follows:

> "A believes that B is planning to attack it. In order to avoid the attack, A makes an explicit commitment to take action against B, should B decide to attack. A's commitment should be such that B is convinced that any action against A will fail, because A has the capacity either to resist or punish B, and to outweigh any prospective gains for B. B's conviction hinges on A's signalling and credibility to act as it threatens. According to this model, we find here the three core elements of deterrence theory: the identification of the opponent (attribution); defence and retaliation as types of deterrence strategies; and the capability of the defender to signal credible threats."[16]

In that sense, attribution is only the first step. However, responsible attribution is not as easy as it seems to be, that is why only the United States, the only superpower used this tool before NotPetya. In the cyberspace, attribution needs both convincing technical evidence and reliable intelligence sources. Due to the anonym and global nature of the Internet, collection of hard evidence from computers and networks is struggling. What can be seen on the defenders' side is only a few technical information or indicators of compromise (IoC). They are usually files and operating system

[16] Mariarosaria Taddeo: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31, no. 3 (2018). 339–355.

activities or source/destination IP addresses. Security researchers should prove who are behind NotPetya by finding evidence in the following infection process:

- dropped files
- process hashes and process privilege checks
- credential theft
- token impersonation
- malware propagation
  - network node enumeration
  - SMB copy and remote execution
  - SMBv1 exploitation via EternalBlue
- UNC write malware to admin$ on remote target
- remote execution of the malware
  - MBR ransomware
  - physical drive manipulation
  - MFT encryption
- file encryption
- system shutdown
- anti-forensics[17]

In case of NotPetya, the EternalBlue vulnerability, used for malware propagation was originated from the National Security Agency in the United States. For credential theft, the attackers used Mimikatz, originally created as a proof of concept by French security researcher Benjamin Delpy in 2011. There was not a complex network infrastructure with millions of previously infected computers in the botnet, as the attack was targeted, originated from the MEDoc update server and it is still not known who and how has hacked this server. In such cases, researchers can only rely on the coding style of the malware. Source codes are similar to fingerprints. A programmer usually has his own coding style, a group of programmers are usually using the same framework to improve their software. Cybercriminals are usually lazy enough to make only minor changes, "feature releases" in different campaigns. But that is not true in case of sophisticated, state sponsored targeted attacks. The name NotPetya was chosen as for first sight, it was similar to Petya ransomware, although it is now obvious, that there is no connection between the two malwares. It is possible that the original source code of NotPetya was stolen or bought from the original author

[17] Karan Sood – Shaun Hurley: NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. *Crowdstrike,* 29 June 2017.

who was convicted by a regional court in Nikopol in the Dnipropetrovsk Oblast of Ukraine to one year in prison in 2018 after pleading guilty to having spread a version of Petya online. He is an unnamed Ukrainian citizen.

NotPetya's traces were well-hidden from the technical perspective. Neither governmental, nor industry sources have uncovered any "smoking guns" that underpins the role of Russia in this cyberattack. However, many countries attributed them with high confidence. We can assume that the United States and maybe other countries had indisputable intelligence information. As Carr wrote:

> "The most likely adversary responsible for a covert attack against those critical systems is an extremist group (religious, political, or anarchist), and the best way to learn which of those groups may have been responsible post-attack is to already have in place a long-term counter-intelligence campaign of infiltration and the development of trusted contacts with access. This cannot be done virtually or from behind a computer. Rather, those intelligence agencies that have yet to devote the bulk of their budget to signals capabilities may be best positioned to tackle the problem of attribution. They understand the need to continue to fund and even expand human intelligence – this is still vital, despite the fact that we are living in the age of Facebook, Twitter and Instagram."[18]

The assumption about the U.S. and allies' capabilities on cyber intelligence against Russia can be confirmed with some examples after NotPetya. We can count such leaked information and direct responses as credible signalling according to the deterrence theory. As Taddeo defines:

> "Signaling can be either general or tailored. General signaling conveys a message about the overall deterrence strategy to the rest of the international arena, through open statements released by a state conveying information about its approaches, commitments, and capabilities. […] Tailored signalling—the conveying of a threat to a specific offender indicating the possible targets of retaliation—is more problematic than general signalling and constitutes a significant obstacle to delivering effective deterrence strategies in cyberspace. This kind of signalling is effective if attribution is certain. If the defender has not identified the offender correctly, tailored signalling can be counterproductive given it may be directed to the wrong actor. Tailored signalling also requires a careful finetuning in order not to expose the defender's capabilities and assets, especially when the defender is considering retaliation in-kind. The risks are multiple and range from exposing knowledge about the opponent's cyber assets, which would imply that the defender has also run cyber operations (sabotage or espionage) against the opponent, to revealing the defender's assets and strategies, which may expose and therefore render futile its cyber capabilities, such as zero-day exploits (for example)."[19]

[18] Jeffrey Carr: Responsible Attribution: A Prerequisite for Accountability. *NATO CCD COE,* 2014.
[19] Taddeo (2018): op. cit. 352.

First of all, on 11 June 2018, the U.S. Department of Treasury's Office of Foreign Assets Control designated five Russian entities and three Russian individuals under Executive Order (E.O.) 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* All property and interests in property of the designated persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.[20]

Some notable cyberattacks can also show how Western countries retaliated Russian cyber (and other military) activities by flashing their capabilities:

- Panama Papers: On 1 April 2016, Mossack Fonseca, Panamanian law firm and corporate service provider notified its customers that millions of digital documents were stolen after a targeted cyberattack. These documents consisted of detailed information about the tax avoidance and money laundry of many notable persons. The hack was committed by an unknown hacker, "John Doe", who said that he had never worked for any intelligence agency. Whether it is true or not, the *Süddeutsche Zeitung* published an interview with Alexey Navalny, head of the Moscow-based NGO Anti-Corruption Foundation on the connection of President Putin and other leading figures with the Panama Papers.
- Dutch intelligence against Cozy Bear: In January 2018, Dutch news sources published a story on how their domestic intelligence service, AIVD accessed the IT system of the Cozy Bear hacker group, that is believed to be associated with Russian intelligence. This group is suspected with many notable cyberattacks, such as attacks during the 2016 Presidential Election.
- Bellingcat and Skripal Poisoners: In 2018 and 2019, Bellingcat, the online investigative journal has published a series of articles about the poisoners of Sergei Skripal and his daughter, who died in the United Kingdom. Based on open source intelligence, they could identify the poisoners and track back their lives even until high school. Although such investigative journalism is highly appreciated, it can be assumed that some kind of official intelligence support was provided by Western countries.
- U.S. cyberattacks on Russian Power Grid: In response to the cyberattacks against its critical infrastructures, the U.S. has conducted a similar attack and shared this information with the press in June 2019. As President Trump's national security adviser, John R. Bolton said, the United States

[20] U.S. Department of Treasury: *Treasury Sanctions Russian Federal Security Service Enablers.* 11 June 2018.

was now taking a broader view of potential digital targets as part of an effort "to say to Russia, or anybody else that's engaged in cyberoperations against us, 'You will pay a price'."

Conclusion

Traditional deterrence theory proposes two potential deterrence strategies: deterrence by defence and by retaliation. In the cyberspace, believing solely in deterrence by defence is not a real option. Simply, because the already developed tools, techniques and procedures set are enormous, and attackers can easily create a previously non-existing attack path. From their point of view, one weak link in the defence chain is enough for success. Therefore, countries should rely more on defence by retaliation, not forgetting to improve their defence capabilities as well. We can see such efforts all over the world.

The EU Cyber Diplomacy Toolbox is an example for that. As the press release of the Council of the EU states:

> "On 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organizations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)."[21]

The lack of EU reaction to NotPetya is a symptom why this Toolbox is necessary. As the relation of the EU members to Russia is complicated, without such common understanding, it is difficult to find a harmonised way for joint sanctions. But states do not forget and forgive. After 5 years of a cyberattack against the German Parliament, Chancellor Angela Merkel seeks EU sanctions as they have hard evidence against Russian actors. This will be the first test of the Toolbox where EU members can prove their willingness for a coordinated response.[22]

> "Cyber-attacks falling within the scope of this new sanction's regime are those which have significant impact and which:

[21] Council of the EU: *Cyber-attacks: Council Is Now Able to Impose Sanctions.* 17 May 2019.
[22] Catherine Stupp: Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament. *The Wall Street Journal,* 11 June 2020.

> – originate or are carried out from outside the EU or
> – use infrastructure outside the EU or
> – are carried out by persons or entities established or operating outside the EU or
> – are carried out with the support of person or entities operating outside the EU
> Attempted cyber-attacks with a potentially significant effect are also covered by this sanction's regime. […] Restrictive measures include a ban on persons travelling to the EU, and an asset freeze on persons and entities. In addition, EU persons and entities are forbidden from making funds available to those listed."[23]

We can see that the U.S. Government is actively using deterrence by retaliation strategy. Currently, it seems to be successful, as since 2017 there was not any major cyberattack, attributed to Russia. However, most of the actions on that field are covert and the public audience will get information decades later. Jason Healey, one the best scholars in this topic and Neil Jenkins tried to measure the success of deterrence from the U.S. perspective. Their article ends with the following thoughts:

> "We can't assess what we don't try to measure. Together, the frameworks in this paper can act as a check on whether these new, riskier U.S. cyber policies and operations are succeeding in suppressing incoming attacks, or inciting them. […] the U.S. Government cannot easily even know all its own operations against adversaries: some will be covert actions, others espionage, while others are "traditional military operations." Each is held in a separate compartment and few individuals have the full picture."[24]

Whatever will happen, the alleged attackers' response will be the same as what we heard from Kremlin spokesman Dmitry Peskov in February 2018, right after the attribution of many countries: "We categorically reject such accusations. We consider them unsubstantiated and groundless. This is nothing but a continuation of a Russophobic campaign that is not based on any evidence."[25]

NotPetya was nor the first, neither the last cyberattack in history. Countries should develop acceptable norms and behaviour in cyberspace, but they are getting farther and farther from a consensus. As both Russia and China can be more independent from the U.S. governed global Internet, as members of the

[23] Council of the EU (2019): op. cit.

[24] Jason Healey – Neil Jenkins: Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Tomáš Minárik – Siim Alatalu – Stefano Biondi – Massimiliano Signoretti – Ihsan Tolga – Gábor Visky (eds.): *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn: NATO CCD COE Publications, 2019. 123–142.

[25] AFP: Kremlin 'Categorically' Denies Russia behind NotPetya Cyber-attack. *France 24,* 15 February 2018.

United Nations Security Council, they are able, and they are willing to influence where the cyberspace is turning. As of 2020, we can see a clear intention from the Western countries to sustain the current situation and remarkable steps from Russia and China towards changing it. Diplomats of the 2020s should notice that what is happening today will have a fundamental effect for the next five decades.

References

AFP: Kremlin 'Categorically' Denies Russia behind NotPetya Cyber-attack. *France 24,* 15 February 2018. Online: www.france24.com/en/20180215-kremlin-categorically-denies-russia-behind-notpetya-cyber-attack

Blumbergs, Bernhards – Tomáš Minárik – Kris Van Der Meij – Lauri Lindström: NotPetya and WannaCry Call for a Joint Response from International Community. *NATO CCD COE,* 2017. Online: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/

Carr, Jeffrey: Responsible Attribution: A Prerequisite for Accountability. *NATO CCD COE,* 2014. Online: https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-6-Carr.pdf

Council of the EU: *Cyber-attacks: Council Is Now Able to Impose Sanctions.* 17 May 2019. Online: www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

Cybersecurity and Infrastructure Security Agency: *Grizzly Steppe – Russian Malicious Cyber Activity.* 16 April 2018. Online: www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

Department of Homeland Security: *Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale.* 30 December 2016. Online: www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary

Foreign and Commonwealth Office: *Foreign Office Minister Condemns Russia for NotPetya Attacks.* 15 February 2018. Online: www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Government Communications Security Bureau: *New Zealand Joins International Condemnation of NotPetya Cyber-attack.* 16 February 2018. Online: www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/

Greenberg, Andy: Petya Ransomware Epidemic May Be Spillover From Cyberwar. *Wired,* 28 June 2017. Online: www.wired.com/story/petya-ransomware-ukraine/

Healey, Jason – Neil Jenkins: Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Tomáš Minárik – Siim Alatalu – Stefano Biondi – Massimiliano Signoretti – Ihsan Tolga – Gábor Visky (eds.): *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn: NATO CCD COE Publications, 2019. 123–142.

Maersk Press Room: *A. P. Moller – Maersk Improves Underlying Profit and Grows Revenue in First Half of the Year.* 16 August 2017. Online: www.maersk.com/press/

press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year
Maynor, David – Aleksandar Nikolic – Matt Olney – Yves Younan: The MeDoc Connection. *Talos Intelligence,* 05 July 2017. Online: https://blog.talosintelligence.com/2017/07/the-me-doc-connection.html
Moret, Erica – Patryk Pawlak: The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? *EUISS,* July 2017. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf
Parliament of Australia: *Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia.* 16 February 2018. Online: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F5793917%22
Republic of Estonia: *Foreign Minister Mikser Condemns Russia for NotPetya Attacks against Ukraine.* 15 February 2018. Online: https://vm.ee/en/news/foreign-minister-mikser-condemns-russia-notpetya-attacks-against-ukraine
Schmitt, Michael N. – Jeffrey Biller: The NotPetya Cyber Operation as a Case Study of International Law. *EJIL:Talk!,* 11 June 2107. Online: www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/
Schmitt, Michael N. – Liis Vihul: International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. *Just Security,* 30 June 2017. Online: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/
Sood, Karan – Shaun Hurley: NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. *Crowdstrike,* 29 June 2017. Online: www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
Stilgherrian: Blaming Russia for NotPetya was Coordinated Diplomatic Action. *ZDNet,* 11 April 2018. Online: www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
Stupp, Catherine: Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament. *The Wall Street Journal,* 11 June 2020. Online: www.wsj.com/articles/germany-seeks-eu-sanctions-for-2015-cyberattack-on-its-parliament-11591867801
Taddeo, Mariarosaria: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31, no. 3 (2018). 339–355. Online: https://doi.org/10.1007/s13347-017-0290-2
The White House: *Statement from the Press Secretary.* 15 February 2018. Online: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/
U.S. Department of Treasury: *Treasury Sanctions Russian Federal Security Service Enablers.* 11 June 2018. Online: https://home.treasury.gov/news/press-releases/sm0410