CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

# CC-DRIVER Policy Brief No. 1

**15 February 2021**

## Who is this for?

The European Commission (REA, DG HOME), selected LEAs, the CC-DRIVER Stakeholder Board, the CC-DRIVER Security Advisory Board and the CC-DRIVER Ethics Advisory Board

## Highlights

1. The Russian SolarWinds attack is a "grave risk" to government and businesses, but no one seems to know the scale of the attack. We have little information on the extent to which European organisations were hacked or what they did about it.
2. We can identify different types of state-sponsored attacks, such as espionage, ransomware, disruption of infrastructure, social disruption and hybrid attacks. Microsoft (and others) have identified the principal attackers as sponsored by Russia, China, Iran and North Korea.
3. There are different policy options on how to respond to such attacks. Doing nothing is not a viable option. If there are no consequences, attackers will continue to spy, steal and attack.
4. Among policy options are naming names, sanctions against the perpetrators, diplomatic isolation, signalling, counterattacks, pre-emptive strikes, demonstrations of power.
5. Policy options are complicated because the US, UK and Israel have engaged in offensive operations too (e.g., Stuxnet). The moral high ground has already been compromised.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

# The Russian hack and EU policy options

**Types of state-sponsored hacks and attacks**

The Russian hack that came to light in December 2020 is just one type of state-sponsored attack. Here are some others:

*Espionage*

The SolarWinds hack has so far been described as an espionage operation, but Microsoft's Brad Smith has said, "This is not 'espionage as usual'... Instead, it represents an act of recklessness that created a serious technological vulnerability for the United States and the world. In effect, this is not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency."[1] The Russians penetrated the e-mail systems of US government agencies. The Chinese have been particularly effective in cyber espionage.

*Ransomware*

A notable example of ransomware was North Korea's WannaCry attack, a money-making operation that froze the computers of the UK National Health Service (NHS), Danish shipping company Maersk, US pharmaceutical Merck, among others, causing billions of dollars in damage.

*Disruption of infrastructure*

The Russians unleashed a botnet against Estonia in 2007 that froze government infrastructure, banks, telecoms, media. In December 2016, the Russians unleashed the Industroyer virus to disrupt Ukraine's energy grid. The malware attacked electricity substations and circuit breakers using industrial communication protocols that are standardised across different types of critical infrastructure, namely power, water, gas, transportation.

*Social disruption*

Attackers sometimes seek to undermine public trust and sow social discord. Such seemed to be the motive prompting hackers to manipulate information stolen from the European Medicines Agency recently. The regulator accused the perpetrators of attempting to undermine trust in vaccines. The Russians were also accused of interfering in the Brexit debates and more notably in the US 2016 presidential election, documented in the Mueller report (2019) which led to the indictment of 12 Russian intelligence agents who were directly engaged in sowing disinformation.

*Hybrid attacks*

Hybrid attacks combine disinformation campaigns with cyberattacks on infrastructure, economic processes and democratic institutions, with the potential for causing physical damage, stealing industrial and state secrets, sowing mistrust, weakening social cohesion and undermining international security.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

**Policy options**

How should the EU, the US and other democratic countries respond to these attacks? Past and ongoing debates in political science and international law have influenced cybersecurity policy and strategy regarding deterrence, the offence-defence balance, involvement of private actors, etc. However, governments have tolerated graver violations and breaches in cyberspace than they would have done in the physical world. Contemporary political and legal cornerstones of our democratic societies need to adapt to the cyber domain. Cybersecurity experts, such as John Carlin, say we need new tools, approaches and ways of thinking about the way that we use traditional geopolitical tools. Responding to and countering attacks oblige policymakers to consider different policy options.

American political scientist Joseph Nye has identified four major means of deterrence in the cyber realm: threat of punishment; denial by defence (making it hard for attackers to overcome defences); entanglement (e.g., China is unlikely to disrupt Western networks in which it has made an investment); and normative taboos (reputation damage). He answers the question of whether deterrence works in cyberspace by explaining that it depends on "who and what".[2]

The EU can consider a range of policy options to respond to state-sponsored hacks and attacks like those by the Russians, Chinese, North Korea and Iran. Among them are these:

*Inaction*

This is not a good option because inaction might be seen as indifference to further attacks and the cost of cyberattacks is growing. The EC's cybersecurity strategy, released in December 2020, notes that two-fifths of EU users have experienced security-related problems and three-fifths feel unable to protect themselves against cybercrime. According to a report by ENISA, there was a 241% increase in the total number of distributed denial of service attacks during Q3 2019 compared with Q3 2018.[3]

The EC has estimated the annual cost of cybercrime to the global economy in 2020 at €5.5 trillion, double that of 2015-16. This represents the largest transfer of economic wealth in history, says the EC, greater than the global drugs trade. For one major incident, the WannaCry ransomware attack in 2017, the cost to the global economy was estimated at over €6.5 billion. [4]

If there is no consequence, attackers will continue to spy, steal and attack.

*Naming names*

The US and the UK have named and published photos of attackers, as the UK did in the case of the Russian agents who poisoned the Skripals. In May 2014, the US named five officers from China's People's Liberation Army for cyber theft of intellectual property. The EU listed six individuals and three entities responsible for, or involved in, cyber-attacks affecting the EU and its Member States in July 2020.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

An evolved form of naming names is naming and shaming, besmirching the reputations of leaders such as Putin and Kim Jong-Un for their excesses and corruptions while their populations suffer great hardships. The notorious public exposure can force states and governments to change their behaviour towards greater accountability.

*Sanctions against perpetrators*

In July 2020, the European Union imposed its first-ever sanctions for cyberattacks on targeting Russian, Chinese and North Korean groups connected to several major hacking incidents. The action, which included travel bans and freezes on individuals and organisations connected to ransomware and industrial espionage, follows earlier sanctions put in place by the United States.[5] Such action embodies Nye's first and second deterrence strategies.

Sometimes, there are uncertainties about to whom to attribute an attack. Punishment is possible against both states and criminals, but attribution problems often slow and blunt its deterrent effects (Nye, p. 68).

*Diplomatic isolation*

Giving a lot of publicity to attacks could help turn other countries against the perpetrating countries like the Russians, Chinese, North Koreans and Iranians. Organising censure votes in international institutions against offending countries could be a possibility in combatting state sponsored cyberattacks.

*Signalling*

The US government has made it publicly clear that it has embedded spyware in Russian energy grids, as the Russians have done in US networks. The action embodies Nye's first deterrent strategy – the threat of punishment. Similarly, the UK has explicitly signalled that it has the capacity to "degrade, disrupt and destroy" its enemies' critical infrastructure in a future cyber conflict.[6]

*Counterattacks*

Attacks and counterattacks risk an escalation in attacks and counterattacks which may quickly aggravate into a war-like situation. Deterrence is far more problematic in cyberspace than it was in the Cold War when it was clear who the warring parties were. In cyberspace, attacks can come from many different directions, from many different sources, from lone wolves to national agencies. It is not always possible to determine who originated an attack (the "attribution problem").

The US uses the phrase "defend forward" to mean that they will go deep into an adversary's computer networks, sometimes to strike back, but more often to signal that an attack will not be cost-free, a combination of policy options that embodies Nye's notion of defence by denial and the threat of punishment.[7]

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

*Pre-emptive strikes*

US intelligence agencies pre-empted the Russian hackers in advance of the 2018 US mid-term elections. The NSA shut down the Internet Research Agency in St. Petersburg for a few days around the 2018 midterms and sent warnings to Russian intelligence officers. The US government and Microsoft reportedly pre-empted a Russian botnet that posed a threat to the 2020 US election.

*Demonstrations of power*

Countries with similar approaches to cyberattacks could build alliances to demonstrate their technological prowess in the attacker's country with a clear message that if the attacker were to attack again, it might suffer serious repercussions longer. A telling example of such demonstrations was when the Russians cut the power in Ukraine for six hours at the outset of its war with that country.

*Détente and refocussing on common challenges*

Is de-escalation of cyberattacks possible? Is it possible to refocus rogue regimes on common existential challenges, e.g., the climate crisis? Such questions embody Nye's entanglement option which focus on easing relations with attacking states. Entanglement and engagement of states in crucial issues of development, environment and health will help in ensuring all states have stakes in avoiding cyberattacks.

*Certification*

The Cybersecurity Act promotes ICT certification at EU level, with a European Cybersecurity Certification Framework for the establishment of voluntary European cybersecurity certification schemes for ICT products, services and processes in the Union.[8] A certification scheme could deny a cybersafe label to products, technologies and services infected with malware and backdoors from Russia, China, North Korea, Iran, Syria and other malign states.

*Multi-pronged responses*

With time and effort, a major military or intelligence agency is likely to penetrate most defences, but the combination of threat of punishment plus effective defence can influence calculations of costs and benefits.[9] None of the four mechanisms of deterrence and dissuasion -- punishment, denial, entanglement, and norms -- is perfect, but together they illustrate the range of means by which it is possible to reduce cyberattacks. [10] As indicated above and in Nye, there are a variety of options for deterrence even in the grey zones of political behaviour that fall below the threshold of armed conflict. Those options include public debate or, as Microsoft has put it: "Talking publicly about nation state attacks is an important part of deterrence."[11]

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

*Make stakeholders part of the strategy*

Businesses may have fewer options than governments who can engage in deterrent operations, but there are still measures they can take. In addition to encouraging and supporting companies to improve their defences and raise staff awareness about social engineering attacks (defence by denial), governments can encourage companies to have better oversight and investigate other suppliers in the value chain and to report to LEAs and CERTs instances in which they have been attacked. While reporting cyberattacks is essential, LEAs and governments must engage stakeholders too in a two-way exchange on the actions to be taken in response to the ongoing attacks.

Governments should promote the role of a Chief Information Security Officer (CISO) and become more transparent about attacks. Microsoft has said it wants "to be transparent and share what we're learning as we combat." There is sometimes a stigma in being a cyberattack victim, but there is more value in sharing information and learning more from each attack.

**Response dilemmas**

Policy options are complicated because intelligence agencies in the US, UK and Israel have engaged in offensive operations too. The Stuxnet malware is a well-known example. Thus, the moral high ground has already been compromised. The choice of options is ultimately a political decision, but as cyberattacks are happening now, and against all of us, all of us need to respond. Unless we show attackers that their attacks will not go unpunished, the attacks will continue. Resilience, fixing vulnerabilities, while necessary, won't stop the attacks. If anything, they only present new challenges to the attackers. Hence, it behoves policymakers, businesses and the public to discuss policy options and reach a consensus on how we should all collaborate in response to the attacks.

# References


[1] https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

[2] Nye Jr., Joseph S., "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3, Winter 2016-17, pp. 44–71 [p. 46].

[3] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, The EU's Cybersecurity Strategy for the Digital Decade, 16 Dec 2020, p. 2.

[4] Ibid., p. 3.

[5] *MIT Technology Review*, "Chinese and Russian hackers were just sanctioned by Europe for the first time", 30 July 2020. https://www.technologyreview.com/2020/07/30/1005822/chinese-and-russian-hackers-were-just-sanctioned-by-europe-for-the-first-time/?truid=1eabd98bb16f6004fa35b14544792a90,%20ec5fc184727f9abde1ba487bc48f7a59&utm_source=weekend_reads&utm_medium=email&utm_campaign=weekend_reads.unpaid.engagement&utm_content=11.28.subs&mc_cid=8a6ad92c0b&mc_eid=331fc6c2f6

[6] Sabbagh, Dan, "Britain has offensive cyberwar capability, top general admits", *The Guardian*, 25 Sep 2020 https://www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits


This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

[7] David E. Sanger, "Accuse, Evict, Repeat: Why Punishing China and Russia for Cyberattacks Fails", *The New York Times*, 22 July 2020. https://www.nytimes.com/2020/07/22/us/politics/china-russia-trump-cyberattacks.html?action=click&module=Top%20Stories&pgtype=Homepage

[8] EU's Cybersecurity Strategy, op. cit., 16 Dec 2020, p. 9.

[9] Nye Jr., Joseph S., "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3, Winter 2016-17, pp. 44–71.

[10] Ibid., p. 66.

[11] Microsoft Digital Defense Report, September 2020, p. 45.

# Further Reading

- Cyberspace Solarium Commission, Report, March 2020. https://www.solarium.gov/
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy, The EU's Cybersecurity Strategy for the Digital Decade, Joint Communication to the European Parliament and the Council, JOIN(2020) 18 final, Brussels, 16 Dec 2020.
- Farrell, Henry, "The political science of cybersecurity", Parts I/II/III/IV/V, *The Washington Post*, 23 Jan 2014. https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/
- Haizler, Omry, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Vol. 1, No. 1, January 2017, pp. 31-45.
- Nye, Joseph S. Jr., "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3, Winter 2016-17, pp. 44-71.
- Straub, Jeremy, "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios", *Technology in Society*, Vol. 59, 2019.
- Terry, Patrick CR, "'Don't Do as I Do' -- The US Response to Russian and Chinese Cyber Espionage and Public International Law", *German Law Journal*, Vol. 19, No. 03, 2018, pp. 613-626.
- Thornton, Rod and Miron, Marina, "Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom", *Journal of Cyber Policy*, Vol. 4, No. 2, 2019, pp. 257-274.



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.