Team: SMINO
Coach: Dr. Fredrik Blix
Students: Daniel Rzhenetskyi
Martin de Jong
Robin Andreasson
Stina Sörman

Cyberattacks Against Essential Services

Simultaneous cyberattacks against hospitals in France and Belgium, and public transport in Germany have undermined normal functionality in those EU member states. Though attribution of the attacks points towards affiliations to ISIS and 'NovAnoN', attribution cannot be confirmed. With vulnerabilities found in large numbers of healthcare systems, together with the coinciding attack against the German transport provider BVG, there is risk of escalation.

As information regarding demands for regaining access to the healthcare systems is missing, the possibility that reducing the functionality of the healthcare system is part of a preparation for a physical attack cannot be excluded. The alternative that the attack against BVG serves as either a diversion, or to finance further attacks should also be taken into account.

The ongoing attack actualises policy issues for how to:

- Compel essential service providers to enhance their resilience;
- Handle ransom demands and attribution in cyberspace;
- Mitigate low-cost, high-impact cyberattacks;
- Distribute information to relevant actors;
- Avoid civil unrest and political turbulence.

Analysis

Healthcare Providers

Incident: A coordinated ransomware attack exploiting known vulnerabilities, disables systems used for medical imaging and patient records at 17 healthcare facilities in Belgium and France. Information regarding demands is lacking.

State: Ongoing - Risk of escalation.
Criticality (healthcare): High
Criticality (EU): Medium
Key Implications:

A. Increased risk of loss of life and jeopardising of health and privacy of individuals.
B. Healthcare facilities across Europe are exposed to the same vulnerabilities.
C. Escalation could impact the national security of EU member states.

The modus operandi seen in the attack against the healthcare facilities is favoured by Al-Durka to generate revenue. The anomalies found in the Bitcoin wallet used for the demanded ransom payment indicate a possible third-party actor. Together with the exposed information on the Marble Framework, developed by the CIA to link malware to a specific developer, it illustrates the complexity of attribution in cyberspace. The Marble Framework could have been further developed and now used to mislead and obscure attribution.

Transport Infrastructure

Incident: NovAnoN claims responsibility for a ransomware attack against BVG´s IT-infrastructure. BVG has met the demand of paying Bitcoins equivalent to €100.000 to regain access.

State: Possibly active and evolving.
Criticality (BVG): Medium
Criticality (EU): Low
Key Implications:

A. Other public transport systems may be compromised.
B. The ransomware could be a smokescreen for further attacks.
C. Having proved to be a lucrative target by paying the ransom, BVG may become the subject of future attacks.
D. The ransom could strengthen the attacker's capability of launching more sophisticated attacks.

The attack against BVG cannot be seen as resolved before integrity of all systems is confirmed. Until such confirmation is made, the possibility that the attack serves as a diversion for an amplified attack should not be discarded, hence deeming the attack as potentially active and evolving. Associations between NovAnoN and the 'Black Bloc' movement potentially indicate spill-over effects of civil unrest into the cyber arena, resembling the development in Estonia 2007.

Martin de Jong
Stina Sörman
Robin Andreasson
Daniel Rzhenetskyy
Coach: Fredrik Blix

Team SMINO
Decision Document
2018-05-21

BLUF

Two attacks on operators of essential services in the EU. One against healthcare facilities in Belgium, France and one against the German public transport operator, BVG. While the ransom has been paid by BVG. information regarding demands against the healthcare facilities is missing.
Cyber Policy Question Presented: How should ransomware attacks against European essential services be tackled?
Objectives: a) Restore functionality of critical infrastructure and vital societal functions, and; **(b)** ensure the trust of operators of essential services throughout the EU.
Goal: To enable long-term opportunities through short-term actions.
Recommendation: PA 4 – Resilience

Policy Alternatives (PAs)

PA1: *Cyber-crime preventive approach with focus on the Rule of Law.*

- Authorities in FR, BE and DE investigate the attacks, with technical support from CERT's and coordination from EC3.
- The cross-border coordination is led by EC3.
- Private actors involved hand over breach information.
- Private actors ensure the integrity of their systems.
- Media is handled by local authorities.

PA2: *Immediate on-site response with the focus on containment and business continuity*

- National CERTs (FR, BE and DE) assist in technical isolation.
- MacGuessin and GR is urged to inform customers about vulnerabilities in their products.
- Task the National Cyber Security Agencies to ensure that sufficient level of security is maintained.
- Meeting demands might be considered only if loss of lives is the direct result of system lock-downs.
- Develop among the affected parties a reliable backup regimen to deter future attacks.
- On EU-level: invest in research on how to make data resistant to silent encryption.
- CERT-EU supports operators of essential services to share information and respond to incidents.
- Brief media that measures have been taken, and the recovery process has begun.

PA3: *Offensive approach with the focus on deterrence*

- The attacks are condemned as an act of terror and demands are rejected.
- Affected states call for NATO consultation (Article 4) to assemble offensive capabilities.
- Intelligence is coordinated and connections between the attacks are investigated.
- Affected hospitals announce that non-critical visits should be avoided.
- GR and MacGuessin are urged to take the lead in resolving the vulnerabilities.
- R&D for offensive capabilities and sectoral strategies for offensive capabilities are encouraged.

PA4: *Resilient approach with the focus on short term effects with long term opportunities*

- Cross-border investigation is led by EC3 and Interpol.
- Affected hospitals increase the state of readiness and call for assistance rather than meeting demands.
- An ad hoc EU software security platform is established.
- Multilateral discussions on cyber threats within the UN and OSCE are promoted.
- All sectors are encouraged to engage in EP3R.
- An EU Cyber Brigade is initiated.
- Need-to-know dialogue with the media is established.

Analysis and Impact of Alternatives

PA1 – Rule of Law: This PA is a cost-effective alternative in proportion to what is yet known. By exercising Rule of Law and holding those behind the attacks responsible without paying a ransom, PA1 gives the opportunity to increase trust in the legal system and strengthen cross-border cooperation. A weakness is that attribution within cyberspace is difficult to determine. Further, PA1 does not prepare for a potential escalation, nor gives any guidelines on how the systems should be fixed. It is however believed that the affected actors will simultaneously patch if they must verify their integrity in cooperation with the vendor.

PA2 – Containment: The strength of this PA is that it focuses on containment and pre-emption, while simultaneously striving for reducing the risk of loss of life. Through the CERT-EU, the operators of essential services in other member states will be warned, which might prevent similar events from happening in other countries. We estimate this as significant, as we cannot correctly attribute at this time, and we are still waiting for the investigation report from BVG. The weakness of this PA is that it is: only effective within member states, non-binding recommendations, requires near total adherence to be effective. Additionally, it does not cover the international cooperation which could be beneficial in case of further escalation. It also might feed the development of ransomware attacks against essential services if the decision to meet the ransom demands was made.

PA3 – Deterrence: This PA has the advantage of increasing the readiness for cyber terrorism and warfare. With its direct and offensive approach, engaging military allies, it could also deter an escalation as well as future attacks. It further gives an opportunity to strengthen the offensive capabilities across NATO and the EU and mark that one does not negotiate with terrorist. However, the alternative acts upon non-confirmed information regarding attribution and does not adequately address the issue of ensuring trust in essential services. As being offensive, it could also encourage rather than deterring escalation and a possible arms race in cyberspace. With its alarming communication, it could fuel political polarisation or attract copycats, as well as civil unrest and weakened trust in essential services.

PA4 - Resilience: PA4 acknowledges the risk of escalation and focuses on mitigating the current state of affairs as well as preparing for future attacks. It takes on several actions aiming at preparing for a potential escalation, while simultaneously increasing the resilience across the EU. When allocating resources to gear up for an escalation, the efforts may be perceived as poorly made investments, if such would not occur. A lack of ownership of the question is also a risk, as the alternative built on cross-border cooperation. However, the alternative aims at converting short-term efforts into synergetic, long-term opportunities and a more effective and coherent cyber response, which all actors will gain from in the future.

Recommendation and Justification

Balancing the aspects of the four policy alternatives, we recommend you to adopt *PA4 - Resilience.* As information regarding attribution and possible demands is lacking, the focus should be put on using the attacks as an opportunity to develop further how the EU and its Member States view and handle cyber security. This crisis could, through extensive collaboration, show the strength of the EU and its international allies rather than the perpetrators. Also, it takes advantage and finds synergies with the regulatory changes in the EU by establishing a framework, to which the NIS Directive and the GDPR can also contribute to an enhanced security for the EU. These actions will enable a better understanding of, and trust in operators of essential services across the EU. Further on, the multilateral discussions within the UN aim at ensuring international support for dealing with the cyber-attacks and will further accentuate EU as a key player in cyber security. If the recent development should escalate, PA4 will ensure that both the affected nations and the EU are prepared and able to act swiftly to minimise any negative impact on our democratic and societal values, as well as defending the EU from simultaneous cyber-attacks.

As the actions taken in PA4 takes on a holistic approach and coordinates actors across national borders and sectors, thus enabling information sharing which will enable opportunities and a positive development of crisis management in the long run.

Team SMINO
Coach: Dr. Fredrik Blix
Competitors: Daniel Rzhenetskyi, Martin de Jong, Robin Andreasson, Stina Sörman
Decision Document
2018-06-19

Ransomware attacks against hospitals in several EU member states. Exploited vulnerabilities are widespread across the interconnected healthcare industry. Attribution is yet not confirmed. Due to the alarming trend of hospitals being subjects to ransomware, the question emerges:

How should the international community respond to ransomware attacks against essential services?

PA1 – International collaboration on the Rule of Law

- INTERPOL coordinates and collect intelligence.
- National CERTs provide support for technical containment to hospitals.
- Conduct criminal investigation against actors inhibiting the Rule of Law
- ENISA launches PPPs for forensic awareness
- Police enhance readiness.

Strength	Weakness
Collected intelligence supports law enforcement investigations.	Evidence collected with questionable collection methods could be dismissed in court.
Opportunity	**Threat**
Potential deterrence of attackers.	Ethical issues arising if innocent people are subject for information collection.

PA2 – Direct on-site response, isolation and triage

- Affected hospitals advised to follow ENISA's guideline for incident management.
- Task the NCSA in member states to assist both affected and non-affected hospitals in other EU countries.
- Offline backups are segregated from other parts of the network; inaccessible to malware infections .

Strength	Weakness
Focuses on triage and containment offering good short- and long-term effects.	Does not cover the international cooperation, which could be beneficial.
Opportunity	**Threat**
Improved on-site capabilities and enhanced resilience.	Ransomware writers will create more sophisticated ransomware.

PA3 – International cooperation against cyber terrorism

- EU Member states assist through Article 222 Lisbon Treaty.
- Affected countries consider NATO Article 5 Collective Defence
- Military interventions may be considered by NATO.
- Public – Private collaboration through NISCP and EU PPPs.
- Media dialogue on a need-to-know basis.

Strength	Weakness
Increase the reediness for hybrid warfare.	Leaving those responding vulnerable to attacks and is limited to the EU-NATO community
Opportunity	**Threat**
Increase transnational cooperation	Securitization and militarisation of the internet

PA4 – International cooperation against hybrid threats

- Affected countries calls for an Article 4 consultation to invoke Article 5.
- Web application checking cryptographic checksums for identifying compromised/vulnerable systems.
- Vendors will provide secured and patched versions of their systems.
- Resources for implementing and maintenance is needed.
- International cooperation and dialogue.

Strength	Weakness
Effective actions for containing the attacks	Does not address how legal issues should be handled
Opportunity	**Threat**
Increase and further develop international collaboration within cybersecurity	International collaboration not guaranteed to give results.

Recommendation

Balancing the aspects of the four policy alternatives, we recommend you to adopt *Policy Alternative 4*. As it is not yet possible to determine the perpetrator of the attacks, focus should be put on investigating the way Nato view and apply Article 5 to the cyber domain. *PA4* offers the best short term solution for ensuring the security of yet unaffected hospitals, it also focus on receiving assistance from NATO instead of Article 222 of the Lisbon Treaty as a measure to relieve pressure on EU nations if the attacks should escalate.

Building on international cooperation and dialogue will allow the inclusion of nations who are not members of EU nor Nato. Such measures could initiate future discussions within the UN and potentially establishing guidelines on how to cope with cyber threats.

Most importantly, *PA4,* addresses the current crisis as well as enabling further international collaboration.

Team SMINO
Coach: Dr. Fredrik Blix
Competitors: Daniel Rzhenetskyi, Martin de Jong, Robin Andreasson, Stina Sörman
Decision Document
2018-06-19

Appendix A

Technical Grounds for PA4

The development and use of:

- Compromise Checker Database (CCDB)
- Digital Forensics Process (DFP) for containment and securing evidence, and
- Action to Regain Healthcare Control and Functionality (RHCF).

The CCDB is a web application based on cryptographic checksum technology for the purposes of identifying compromised or vulnerable medical systems throughout the EU.

Compromised systems are then subjected to a *Digital Forensics Process* directed by experts at local police agencies. This process aims at containing the attack by system shutdown except for treatment systems whose network traffic is instead controlled. Systems media such as hard drives is either removed or forensic images are made of them for criminal investigation.

Finally, vendors, through the *Regain Healthcare Control and Functionality* action, provide secured and patched versions of their systems through a read-only web page available to hospitals. They also provide installation advice. Treatment systems installation images come with already basic configuration made so that basic functionality can be regained directly after reinstallation.