CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Escalation Roadmap: An analysis paper

Lieutenant Colonel Ben Valk

**NATO Cooperative
Cyber Defence Centre Of Excellence**

About the author

Lieutenant Colonel Ben Valk is a researcher of the Law Branch of the CCDCOE. Before joining the CCDCOE he has held several positions in the Royal Netherlands Air Force and served as deputy legal adviser of the International Military Staff of NATO Headquarters in Brussels. He has been deployed in international missions in Iraq and South Sudan, serving as senior legal advisor.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from the military, government, academia and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. It encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability across its closely connected focus areas of technology, strategy, operations and law.

The *Tallinn Manual*, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT-systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE also hosts the International Conference on Cyber Conflict (CyCon), a unique annual event in Tallinn, bringing together key experts and decision-makers from the global cyber defence community. The conference, which has taken place in Tallinn each spring since 2009, attracts more than 600 participants.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO CCDCOE. It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Table of Contents

1. Abstract

Discussing the stability of cyberspace to ensure a stable and peaceful cyberspace is an important but leaves open the question of what action nations should take if things go wrong, what cyber activities would constitute a crisis and when nations should inform and involve the United Nations (UN). This analysis tries to create an escalation roadmap that can be used to decide if a malicious cyber activity or attack should lead to the involvement of the UN, European Union (EU) or the North Atlantic Treaty Organization (NATO).

2. Introduction

On 22 May 2020 at the instigation of Estonia during its presidency of the UN Security Council, in an informal meeting 'the SC for the first time discussed the stability of cyberspace as a separate subject'.[1] The meeting 'focused on conflict prevention and ensuring a stable and peaceful cyberspace. The focus was on raising the awareness of members of the UN Security Council about cyber threats against international peace and security and the mechanisms supporting and regulating responsible state behaviour at the global, regional and national level. The meeting allowed states to share their experiences on the application of international law and cyber norms in cyberspace, on which regional cooperation formats have been successful in ensuring cyber stability and identifying cyber threats'.[2]

Discussing the stability of cyberspace to ensure a stable and peaceful cyberspace is an important step, but leaves open the question of what action nations should take if things go wrong, what cyber activities would constitute a crisis and when should nations inform and involve the UN.[3]

This analysis focussed on the definition as mentioned Oxford English Dictionary (OED) definition, literature and Estonian legislation. A crisis would at least have an event or chain of events that cause danger or threats and need urgent or prompt actions to deal with it. For the events, Estonian legislation mentions interruption of a vital service, danger to life or health, environmental damage or severe and extensive interference with the continuity of vital services. Using the groups of threats mentioned in the European Union Agency for Cybersecurity (ENISA 2022 report[4] it can be concluded that there is an overlap in the described threats that could cause the events mentioned in the Estonian legislation. However, it is the effect caused by the threat rather than the threat itself which is decisive in concluding whether it constitutes a crisis. Based on the five groups of harms described in the 'Taxonomy of cyber-harms'[5] there must be a certain level of harm required to constitute a malicious cyber event or attack becoming a crisis.

Focussing on the UN and crisis management, only when a cyber operation reaches the level of an armed attack and a state exercises its inherent right of self-defence under Article 51 of the UN Charter should an event be reported to the Security Council. In other situations where a nation does not have the capacity to respond to a sudden-onset crisis or substantial deterioration of a humanitarian situation triggered by natural and human-induced hazards or conflict, it can request UN support. As criteria, scale, complexity, urgency, capacity and risk of failure to deliver humanitarian assistance at scale to affected populations are cited[6]. It is a national prerogative to decide to report to the UN and ask for assistance and such a decision would have to be made on a case-by-case basis.

Looking at NATO, a NATO member nation could ask for Article 4 discussions when it believes its territorial integrity, political independence or security is threatened. The North Atlantic Treaty and the NATO crisis management process show that there is no obligation for a NATO member nation to report to or involve NATO when a malicious cyber activity or attack constitutes a crisis. However, if such a situation occurs it is unlikely that a member nation would not inform NATO or ask for help. When a malicious cyber activity or attack reaches the level of an armed attack, the member nation can request invocation of Article 5 of the treaty.

According to the network and information systems (NIS)2[7] directive, malicious cyber operations and attacks are cybersecurity incidents. When the disruption caused by these reaches a level that is too extensive to handle for a single

[1] https://un.mfa.ee/estonia-in-the-security-council-the-first-year/ 'Informal meeting on cyberstability and conflict prevention'.

[2] Ibid

[3] Note that the decision on when to involve the UN would be based on circumstances at the time of the activity of attack. This analysis paper will not give a black and white rule.

[4] ENSIA Threat Landscape 2022.

[5] A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate' page 7, Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese and David Upton, Journal of Cybersecurity, 16 October 2018.

[6] Humanitarian System-Wide Scale-Up Activation Protocol 1: Definition and Procedures, endorsed by Endorsed by IASC Principals, November 2018, https://interagencystandingcommittee.org/iasc-transformative-agenda/content/iasc-protocol-1-humanitarian-system-wide-scale-activation

[7] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)', 14 December 2022.

member state or when two or more member states are affected with such a wide range of technical or political difficulty that it requires timely coordination and response at the NATO political level, the incident has to be reported.

To visualise the options when a malicious cyber operation or attack occurs, a flowchart has been created that can be used to determine if an incident has to be reported. An additional flowcharts show possible response options when a malicious cyber activity does not lead to the involvement of international entities.

3. Cyber operations and attacks that constitute a crisis

The United Nations Office for Disaster Risk Reduction (UN UNISDR) Terminology on Disaster Risk Reduction states that a 'crisis or emergency is a threatening condition that requires urgent action',[8] but there is no exploration whether cyber operations or attacks could constitute a crisis. The Oxford English Dictionary (OED) defines a crisis as a 'time of great danger, difficulty or doubt when problems must be solved or important decisions must be made'.[9] Other literature states that a crisis is a 'serious threat to the basic structures or the fundamental values and norms of a social system, which – under time pressure and highly uncertain circumstances – necessitates making critical decisions'.[10] The Estonian Emergency Act does not define crisis but offers a definition of an emergency:

> An emergency is an event or a chain of events or an interruption of a vital service which endangers the life or health of many people, causes major proprietary damage, major environmental damage or severe and extensive interferences with the continuity of vital services and resolution of which requires the prompt coordinated activities of several authorities or persons involved by them, the application of a command organisation different from usual and the involvement of more persons and means than usual.[11]

The OED defines an emergency as a 'sudden serious and dangerous event or situation that needs immediate action to deal with it'[12] and so both crisis and emergency have similar elements. Each contains an event or chain of events that causes danger or threats and needs urgent or prompt actions to deal with it. The question is how this would translate to cyber activities or attacks.

The UN recognises existing and emerging information and communications technologies (ICT) threats but does not have a definition.[13] The EU defines a cyber threat as 'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons'[14] The ENISA divides these threats into 7 groups: ransomware; malware; social engineering threats; threats against data; denial-of-service; threats against availability; and internet threats such as disinformation, misinformation and supply chain attacks (Figure 1).[15] It will be the effect of these threats and whether they would lead to an interruption of a vital service, danger to life or health, environmental damage or severe and extensive interferences with the continuity of vital services that would determine whether the threat could lead to a crisis or not. As there is no agreed subdivision of threats, in this paper the subdivision by ENSIA (Figure 1) will be used to analyse whether a threat could lead to a crisis.

[8] 2009 UN UNISDR Terminology on Disaster Risk Reduction, page 13, May 2009.

[9], Oxford Learner's Dictionaries, https://www.oxfordlearnersdictionaries.com/definition/english/crisis_1?q=crisis.

[10] Crises and Crisis Management: Toward Comprehensive Government Decision Making 277, Uriel Rosenthal and Alexander Kouzmin, J-PART.

[11] Estonian Emergency Act, §2. (1), passed 08.02.2017, https://www.riigiteataja.ee/en/eli/513062017001/consolide.

[12] https://www.oxfordlearnersdictionaries.com/definition/english/emergency?q=emergency.

[13] Group of Governmental Experts (GGE) 2021 report, Chapter II, Open-ended working group, paragraph -23.

[14] Article 2, point (8), of Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU), 17 April 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881.

[15] ENSIA Threat Landscape 2022, October 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport.

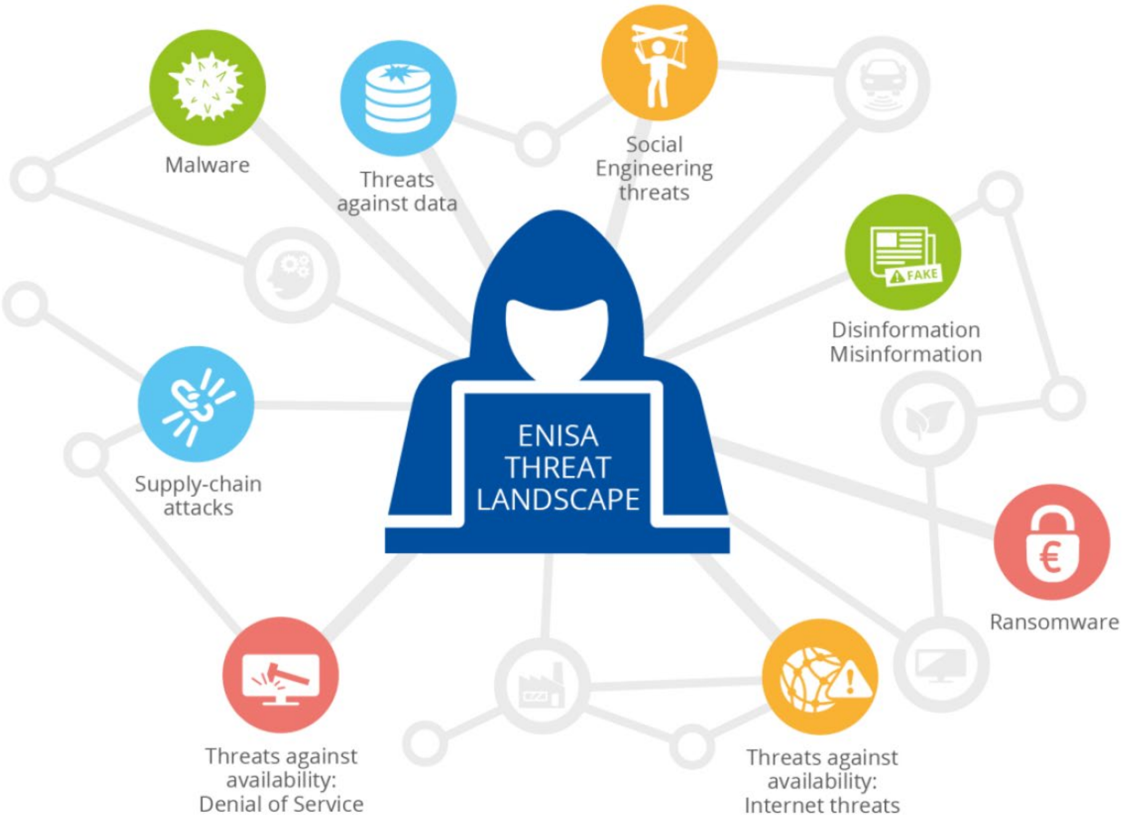

Malware
Threats against data
Social Engineering threats
Disinformation Misinformation
FAKE
Supply-chain attacks
ENISA THREAT LANDSCAPE
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

Figure 1: ENISA Threat Landscape 2022 - Prime threats[16]

Ransomware. Ransomware is defined by the ENISA as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability.[17] Malware encrypts data and renders it unavailable unless a demand is met. In itself, ransomware does not directly lead to the aforementioned effects. However, if data from a hospital is encrypted it could lead to a danger to life, especially if medical information cannot be accessed in times of emergency. This could lead to national action.[18] Ransomware could also have an economic effect if parts of the distribution system are attacked. Maersk reported losing up to $300 million as a result of the NotPetya malware.[19] The average cost of a ransomware attack according to IBM, not including the cost of the ransom itself, was $4.54 million.[20]

Malware. Malware, also referred to as malicious code or malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will harm the confidentiality, integrity or availability of a system.[21] Malware could lead to disruption to a computer, server, client or computer network, leak private information, gain unauthorised access to information or systems, deprive access to information or unknowingly interfere with the user's computer security and privacy. Researchers tend to classify malware into

[16] Ibid page, 10.

[17] Ibid, page 8.

[18] On the Friday morning of May 17 2021 the National Health System (NHS) of the UK was attacked and the same day, NHS England declared a national major incident, Lessons learned review of the WannaCry Ransomware Cyber Attack, NHS Improvement, Smart, Department of Health & Social Care, , August 2018.

[19] The Cost of a Malware Infection? For Maersk, $300 Million, Digital Guardian, 7 August 2020, The Cost of a Malware Infection? For Maersk, $300 Million (digitalguardian.com).

[20] Cost of a Data Breach Report 2022, a IBM study looking at 550 organizations impacted by data breaches that occurred between March 2021 and March 2022. The breaches occurred across 17 countries and regions and in 17 different industries, IBM July 2022, 3R8N1DZJ (ibm.com).

[21] ENSIA Threat Landscape 2022, October 2022, page 8.

one or more sub-types: viruses, worms, Trojan horses, ransomware,[22] spyware, adware, rogue software, wiper and keyloggers).[23] The variation in types of malware also shows the possible results. Spyware could lead to information about individuals or an organisation being sent to another entity and therefore violating privacy or endangering the device's security. In the General Data Protection Regulation (GDPR), a personal data breach is defined 'as any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed'.[24] Privacy is of concern, but the leak of personal information could also lead to risks for those whose data is disclosed. Following the Taliban takeover in Afghanistan in 2021, the group gained control over biometric systems containing highly sensitive data that Western donor governments left behind, including iris scans, fingerprints, photographs, occupation, home addresses and names of relatives. The Taliban could use them to target perceived opponents, and Human Rights Watch research suggests that they may have already used the data in some cases.[25] In early 2022, a highly targeted cyber attack against the International Committee of the Red Cross (ICRC) was detected. It compromised the sensitive data of more than 515,000 people, including names, locations and contact information of missing persons, detainees and other highly vulnerable people affected by a humanitarian crisis.[26] Other malicious software that interferes, disrupts or even wipes supervisory control and data acquisition (SCADA) systems of critical national infrastructure (CNI) can also create effects that would lead to a crisis. As an example, malware that disrupts a water treatment facility in such a way that drinking water is polluted might lead to a crisis.[27]

Social engineering. Social engineering encompasses a broad range of activities that attempt to exploit human error or behaviour to gain access to information or services.[28] It is not a direct cyber activity[29] but lures users into opening documents, files or e-mails, visiting websites or granting unauthorised access to systems or services and always needs a human element to be successful. Depending on the effect of the hacker's actions after access to the information or service, it could lead to a crisis but the activity itself does not.

Threats against data. Threats against data form a collection of threats that target sources of data with the aim of gaining unauthorised access and disclosure, as well as manipulating data to interfere with the behaviour of systems[30]. Disclosure of personal, sensitive or classified data could be a GDPR violation or bring a government into disrepute.[31] As described under the malware paragraph, manipulating data could lead to serious effects if it involved CNI.

Threats against availability: Denial of Service. Availability is the target of a plethora of threats and attacks, among which distributed denial-of-service (DDoS) stands out.[32] Ransom denial-of-service (RDoS) is the new frontier of denial-of-service attacks. RDoS aims to identify vulnerable systems that become the target of the attack and put in place different activities that result in a final request to pay a ransom. RDoS can come in two

[22] Note that the ENSIA Threat Landscape 2022, October 2022, page 8, describes ransomware as a separate threat.

[23] Malware, Wikipedia, https://en.wikipedia.org/wiki/Malware.

[24] Article 4.12 GDPR. https://gdpr-info.eu/.

[25] Human Rights Watch (2022). New Evidence that Biometric Data Systems Imperil Afghans, 30 March 2022.

[26] International Committee of the Red Cross (2022). Cyber- Attack on ICRC: What We Know, 16 February 2022.
April 2022.

[27] A Murderous Cyber-Attack Is Only A Matter Of Time, Shashank Joshi (2020), The Economist, 17 November 2020; Global Water Intelligence (2021). Mekorot Continues Efforts To Secure Its Critical Infrastructure Against Cyber-Attacks, 1 July 25021; Florida Water Treatment Plant Hit With Cyber Attack, Steve Kardon, Industrial Defender, 9 February 2021.

[28] ENSIA Threat Landscape 2022, October 2022 page 8, https://www.imperva.com/learn/application-security/social-engineering-attack/.

[29] Wikipedia, Social engineering (security) - Wikipedia.

[30] ENSIA Threat Landscape 2022, October 2022 page 8

[31] Hackers Breach U.S. Marshals System With Sensitive Personal Data, New York Times, 27 February 2023 https://www.nytimes.com/2023/02/27/us/politics/us-marshals-ransomware-hack.html.

[32] ENSIA Threat Landscape 2022, page 69, October 2022.

flavours: attack first or extortion first. In the former, a DDoS attack is implemented and a ransom is demanded to stop it. In the latter, an extortion letter and proof in the form of a small-scale DoS attack are sent with a ransom demand.[33] The internet threats group covers threats that have an impact on the availability of the internet, such as border gateway protocol (BGP) hijacking.[34] As both of the threats do not result in permanent damage, it would be unlikely that these would result in a crisis.

Disinformation and misinformation. Disinformation and misinformation campaigns are still on the rise, spurred by the increased use of social media platforms and online media. Disinformation is an intentional attack that consists of the creation or sharing of false or misleading information.[35] Misinformation is an unintentional attack, where sharing of information is done inadvertently. Inaccuracy carried by the information is unintentional and could happen for example when a journalist reports wrong information in good faith or reports information by mistake.[36] Disinformation can lead to a crisis if a disinformation campaign would have the intent to destroy in part or in whole a national, ethnical, racial or religious group.[37] Radio Télévision Libre des Mille Collines played a significant role in inciting the Rwandan genocide in 1994[38] and a Facebook campaign was launched against the Rohingya minority in Cambodia.[39]

Supply Chain Attacks. A supply chain attack targets the relationship between organisations and their suppliers. Microsoft states that 'supply chain attacks are an emerging kind of threat that target software developers and suppliers. The goal is to access source codes, build processes or update mechanisms by infecting legitimate apps to distribute malware'.[40] ENISA defines where an attack is considered to have a supply chain component when it consists of a combination of at least two attacks.[41]

Looking at the ENSIA list of cybersecurity threats it is clear that there is an overlap. Ransomware could also be classified as malware. Availability of data could be compromised by DDoS attacks, but also wiper ware. This leads to the conclusion that threats are not the best ways to conclude whether a malicious cyber activity or attack would lead to a crisis.

In line with the description of a crisis it is better to look at the effects or harm of the malicious cyber activity or attack to decide whether it constitutes a crisis. The 'A taxonomy of cyber-harms' article[42] divides cyber-harms types into categories:

- Physical or Digital harm (i.e. harm describing a physical or digital negative effect on someone or something).

- Economic harm (i.e. harm that relates to negative financial or economic consequences).

[33] Ibid, page 73.

[34] Ibid, page 79.

[35] ENSIA Threat Landscape 2022, October 2022 page 9.

[36] Ibid, page 9.

[37] See Article II of the UN Genocide Convention 'G*enocide means any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such: (a) Killing members of the group; (b) Causing serious bodily or mental harm to members of the group; (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; (d) Imposing measures intended to prevent births within the group; (e) Forcibly transferring children of the group to another group.".*

[38] Wikipedia, Radio Télévision Libre des Mille Collines..

[39] A Genocide Incited on Facebook, With Posts From Myanmar's Military, New York Times, 15 October 2018 Myanmar: The social atrocity: Meta and the right to remedy for the Rohingya, Amnesty International, 29 September 2022; Facebook asked to clarify role in fuelling 'Rohingya genocide', Phnom Penh Post, Mar 9, 2022.

[40] Microsoft, Supply chain attacks, 2 February 2023

[41] 'A supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets', ENISA Threat Landscape for Supply Chain Attacks page 7, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[42] 'A taxonomy of cyber-harms', page 7.

- Psychological harm (i.e. harm which focuses on an individual and their mental well-being and psyche).
- Reputational harm (i.e., harm pertaining to the general opinion held about an entity).
- Social and Societal harm (i.e., a capture of harms that may result in a social context or society more broadly).[43]

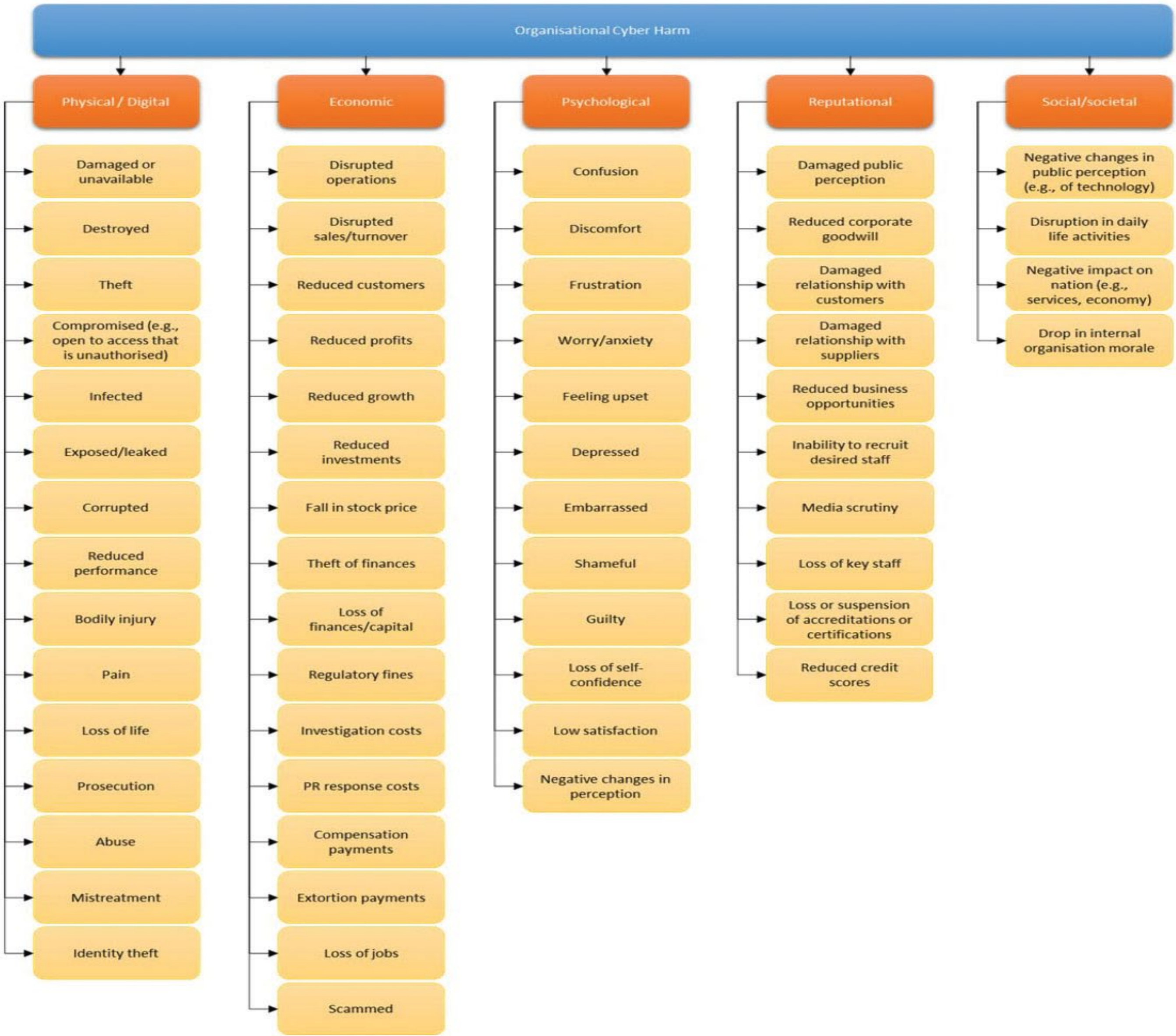


Figure 2[44]

There are five broad categories.

Physical or digital harm. Malicious cyber activities or attacks that result in physical or digital harm could constitute a crisis. Digital harm would concern the confidentiality, integrity or accessibility of data. Examples would be exfiltration or theft of sensitive or customer data, corrupted data files or unavailable systems. Depending on the results, these could also lead to physical harm, meaning bodily injury or physical damage. The attack on the National Health System of the UK disrupted the system but could have led to danger to life and health. Malware affecting SCADA systems on CNI or other industrial systems could lead to real damage

[43] Ibid, page 7.

[44] Ibid, page 8.

like in the Stuxnet case or the cyber attack on a steelworks in Germany.[45] Depending on the scale and effect,[46] these could lead to a crisis.

Economic harm. Depending on the scale and effect, malicious cyber activity or an attack could lead to a crisis. A DDoS attack leaving the site of a bank unavailable for a few hours would be disruptive but does not constitute a crisis. Attacks like the NotPetya attack had great logistic effects[47] and caused the radiation monitoring system at Ukraine's Chornobyl nuclear power plant to go offline[48] could be considered a crisis, but no crisis was declared. The Colonial Pipeline ransomware attack that led to the 'shut down of the pipeline as a precaution'[49] resulted in a fuel shortage that caused rising fuel prices[50] and delays in air traffic and the Governors of Georgia,[51] Louisiana,[52] North Carolina[53] and Virginia[54] declared a state of emergency.

Psychological harm is focused on the 'mental well-being and psyche of the individual'[55] therefore it would be logical to conclude that this would not constitute a crisis. However in the article 'Cyberattacks, Psychological Distress and Military Escalation: An Internal Meta-Analysis'[56] scholars 'using a powerful meta-analytic technique' concluded that 'cyberattacks cause significant psychological harm equivalent to the distress elicited by major terror events'.[57] They conclude 'that exposure to cyberattacks can (although not necessarily) cause sufficiently severe mental suffering to qualify as an armed attack and trigger the right of self-defence'.[58] As an example, they refer to the Iranian cyber attacks against Albania, during which Albania considered invoking NATO's Article 5.[59] These attacks 'destroyed government data and disrupted government services to the public'.[60] The authors state that 'psychological harm following cyberattacks shifts public opinion. Second, shifts in public opinion influence national decision-making'.[61] Based on this it is imaginable that psychological harm caused by a malicious cyber activity or attack could constitute a crisis.

Reputational harm. Malicious cyber activities and attacks could result in reputational harm to governmental and non-governmental entities. The Federal Reserve System (FED), the central bank of the United States (US), recognises that 'weaknesses in a firm's controls, defences and recovery ability can allow cyber events to become cyber incidents, impairing operations (for example, by causing a loss of funds or data; corrupting data; halting operations; or causing other monetary or reputational losses'.[62] A malicious cyber activity like the hack on the US Marshals system where sensitive data 'included a trove of personal information about investigative

[45] Stuxnet, Stuxnet - Wikipedia, BBC news, "Hack attack causes 'massive damage' at steel works", (22 December 2014), BBC.

[46] See also TM rule 69, Definition use of Force; Rule 71. Self-defence against an armed attack.

[47] Shipping company Maersk says June cyberattack could cost it up to $300 million, CNBN, 16 August 2012, 'The Maersk cyber attack - how malware can hit companies of all sizes', Hilary Walton, 11 September 2022.

[48] "Chernobyl's radiation monitoring system has been hit by the worldwide cyber attack", The Independent, 27 June 2017.

[49] Colonial Pipeline ransomware attack, Wikipedia.

[50] 'Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack', Vanessa Romo, NPR, 11 May 2021.

[51] 'Carr: Kemp Declares State of Emergency due to Colonial Pipeline Cyber Incident, Invokes Price Gouging Statute', Office of the Attorney-General of the State of Georgia, 11 May 2021.

[52] 84 JBE 2021 State of Emergency - Colonial Pipeline.pdf ' proclamation number JBE 2021-84', State of Louisiana (12 May 2021).

[53] 'Executive Order No. 213', State of North Carolina, 10 May 2021.

[54] 'Executive Order Number Seventy-Eight (2021)', Office of the Governor of the Commonwealth of Virginia 11 May 2021.

[55] 'A taxonomy of cyber-harms', page 7.

[56] 'Cyberattacks, Psychological Distress and Military Escalation': An Internal Meta-Analysis, Ryan Shandler, Michael L Gross, Daphna Canetti, Journal of Global Security Studies, Volume 8, Issue 1, March 2023.

[57] Ibid, page 15.

[58] Ibid, page 13.

[59] 'Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack'. Politico, 5 October 2022.

[60] Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania, White House, 07 September 2022.

[61] 'Cyberattacks, Psychological Distress and Military Escalation': An Internal Meta-Analysis, page 14.

[62] Implications of Cyber Risk for Financial Stability, FED, 12 May 2022.

targets and agency employees'[63] was retrieved would affect people's trust in governmental institutions. Reputational harm could lead to activities like a bank run and therefore constitute a crisis.

Social and societal harm will include malicious cyber activities like disinformation campaigns. With the outbreak of COVID, disinformation was spread by several entities, undermining the trust in the government-led approach to fight the pandemic.[64] Attacks on CNI will disrupt daily life and change the public perception of technology. Disinformation can spark events as was shown by the 6 January attacks on Capitol Hill.[65]

A crisis would at least have the following elements: an event or chain of events that cause danger or threats and need urgent or prompt actions to deal with them. For the events, Estonian legislation mentions interruption of a vital service, a danger to life or health, environmental damage or severe and extensive interference with the continuity of vital services. Using the groups of threats mentioned in the ENISA 2022 report[66] it can be concluded that there is an overlap in the described threats that could cause the events mentioned in the legislation. However, it is the effect caused when the threat materialises that is decisive for determining whether it constitutes a crisis and not the event itself. Based on the five groups of harms described in the 'Taxonomy of cyber-harms' [67] there must be a certain level of harm to conclude whether a malicious cyber event or attack constitutes a crisis. As there is no general rule on which harm constitutes a crisis, such a decision has to be taken on a case-by-case base.

[63] 'Hackers Breach U.S. Marshals System With Sensitive Personal Data', New York Times, 27 February 2023.

[64] 'Misinformation on COVID-19: what did we learn?', EU knowledge hub, 21 February 202.

[65] 'Election misinformation helped fuel the Jan. 6 Capitol attack. Now, climate misinformation threatens the planet', Washington Post, 6 January 2022; 'Facebook Hosted Surge of Misinformation and Insurrection Threats in Months Leading Up to Jan. 6 Attack', Craig Silverman ProPublica, Craig Timberg The Washington Post, Jeff Kao ProPublica, and Jeremy B. Merrill, The Washington Post, 4 January 2022.

[66] ENSIA Threat Landscape 2022.

[67] 'A taxonomy of cyber-harms, page 7.

4. Crisis management in the UN

On 26 June 1945, the representatives of the 50 countries signed the UN Charter. On 24 October after ratification by the five permanent members of the Security Council and a majority of the other signatories, the UN officially came into existence. It was founded:

> to maintain international peace and security and to that end: to take effective collective measures for the prevention and removal of threats to the peace and for the suppression of acts of aggression or other breaches of the peace and to bring about by peaceful means and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.[68]

The UN will play a role in crisis management where it could influence international peace and security. This analysis will focus on cyber operations and attacks that constitute a crisis and not on cyber activities that rise to a level of an armed attack where a state may exercise its inherent right of self-defence according to Article 51 of the UN Charter and 'measures taken by members in the exercise of this right of self-defence shall be immediately reported to the Security Council'.[69] Under Articles 41 and 42 of the Charter, the Security Council:

> can determine that a cyber operation constitutes a threat to the peace, breach of the peace or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures.[70]

This can be done without any member reporting to the UN.

To decide which cyber operation constitutes a crisis and when nations should involve the UN, it is necessary to define a crisis. The 2009 UN International Strategy for Disaster Reduction (UNISDR) Terminology on Disaster Risk Reduction states that a 'crisis or emergency is a threatening condition that requires urgent action'.[71] Examples of crises are given on the UN Crisis Relief website.[72] The UN Crises Relief office is run by the UN Office for the Coordination of Humanitarian Affairs (OCHA). On the OCHA website there is no reference to a crisis definition, but activities of the OCHA Inter-Agency Standing Committee (IASC) are described. The IASC is the longest-standing and highest-level humanitarian coordination forum of the UN created by General Assembly resolution 46/182.[73] The Resolution states that "humanitarian assistance is of cardinal importance for the victims of natural disasters and other emergencies'.[74] It goes on that 'the sovereignty, territorial integrity and national unity of states must be fully respected in accordance with the Charter of the UN. In this context, humanitarian assistance should be provided with the consent of the affected country and in principle based on an appeal by the affected country'.[75] It is only in Article 10 that the word crisis is mentioned. 'Many emergencies reflect the underlying crisis in development facing developing countries'.[76] However, this does not relate to a natural disaster or emergency as described in Article 1 but to the underlying causes.

[68] UN Charter Article 1(1).

[69] Ibid Article 51, Tallinn Manual, rule 71.

[70] Tallinn Manual, rule 76.

[71] 2009 United Nations International Strategy for Disaster Reduction (UNISDR) Terminology on Disaster Risk Reduction, page 13, May 2009, https://reliefweb.int/attachments/23d1b19f-83b9-3d9b-b576-fb6edabcd923/Full_Report.pdf.

[72] https://crisisrelief.un.org/.

[73] General Assembly resolution 46/182, 19 December 1991 https://interagencystandingcommittee.org/system/files/legacy_files/GA%20RES%2046-182.pdf.

[74] Ibid Article 1.

[75] Ibid Article 3.

[76] Ibid Article 10.

The IASC Protocol 1. Humanitarian System-Wide Scale-Up Activation[77] states that 'the IASC Principals have agreed that major sudden-onset crises and/or substantial deterioration of a humanitarian situation triggered by natural and human-induced hazards or conflict, which require system-wide mobilization are to be subject to a Humanitarian System-Wide Scale-Up Activation'.[78] It goes on that 'Specifically, an IASC Scale-Up activation is a system-wide mobilization in response to a sudden onset and/or rapidly deteriorating humanitarian situation in a given country, including at the subnational level, where the capacity to lead, coordinate and deliver humanitarian assistance does not match the scale, complexity and urgency of the crisis'. The scale-up activation shall be issued 'on the basis of an analysis of the following criteria: scale, complexity, urgency, capacity and risk of failure to deliver humanitarian assistance at scale to affected populations'.[79] These documents recognise crisis and crisis response measures as IASC Scale-Up activation but none of these are related to malicious cyber activities or attacks. In an overview paper produced by UN OCHA[80] the humanitarian implications of cyber threats are recognised but in none of these documents is an obligation to report or involve the UN when a crisis occurs created.

The UN OEWG 2021 and the GGE 2021 reports both recognise existing and emerging ICT threats. Both recommend establishing a point of contact (PoC)[81] for the exchange of information as part of confidence-building or cooperative measures. Neither report creates an obligation to report to or involve the UN. Information on cyber incidents will be shared voluntarily.

Only when a cyber operation reaches the level of an armed attack and a state exercises its inherent right of self-defence under Article 51 of the UN Charter should this be immediately reported to the Security Council. In other situations where a nation does not have the capacity to respond to a sudden-onset crisis or substantial deterioration of a humanitarian situation triggered by natural and human-induced hazards or conflict, it can request the UN for support. The criteria could be scale, complexity, urgency, capacity and risk of failure to deliver humanitarian assistance at scale to affected populations. It is a national prerogative to decide to report to the UN and ask for assistance and such a decision would have to be made on a case-by-case basis.

[77] Humanitarian System-Wide Scale-Up Activation Protocol 1: Definition and Procedures, endorsed by Endorsed by IASC Principals, November 2018, https://interagencystandingcommittee.org/iasc-transformative-agenda/content/iasc-protocol-1-humanitarian-system-wide-scale-activation.

[78] Ibid, Article 1.

[79] Ibid, Article 1.

[80] 'Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats', UN OCHA, 2022.

[81] GGE, 2021 report 76-78, OEWG 2021 report 47, 51.

5. NATO and crisis management

NATO is a political and military alliance of 31 nations. Founded in 1949 by the signing the North Atlantic Treaty,[82] the fundamental role of the Alliance is to 'guarantee the freedom and security of its member countries by political and military means'.[83] Each day member countries consult each other and take decisions on security issues at all levels and in a variety of fields.[84] All NATO decisions are made by consensus after discussion and consultation among member countries.[85] The 2022 strategic concept[86] describes the key purpose of NATO 'to ensure our collective defence, based on a 360-degree approach'[87] and its core tasks 'deterrence and defence, crisis prevention and management and cooperative security'.[88] The cornerstone of the Alliance is Article 5 of the North Atlantic Treaty:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
>
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.'

In 2014 NATO recognised that a cyber attack could reach the threshold of an armed attack and a 'decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis'.[89] The 2021 Brussels Summit Communiqué stated that 'Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack'.[90]

There are malicious cyber activities that do not reach the level of an armed attack but could be considered a crisis. NATO defines a crisis as a 'disruption of the equilibrium within a nation or among several nations, creating tensions which might lead to serious turmoil or to a conflict'.[91] As NATO recognises the sovereignty of its member states, each would have to report to NATO if it considers its internal equilibrium to be disrupted. This could be a so-called Article 4 consultation where a nation could request consultation because it considers its territorial integrity, political independence or security of a nation is threatened. Since the Alliance's creation in 1949, Article 4 has been invoked seven times[92] indicating that the bar for a member country to formally invoke Article 4 is high.

Besides Article 4 consultations, formal and informal consultation takes place continuously and at different levels. The North Atlantic Council (NAC) meets every week at ambassadorial level.[93] The Military Committee (MC), the senior military authority in NATO and the oldest permanent body in NATO after the NAC, also meets weekly at the level of

[82] 'The North Atlantic Treaty', Washington D.C., 4 April 1949.

[83] 'NATO Checklist', www.nato.int.

[84] 'What is NATO?' www.nato.int.

[85] 'Consensus decision-making at NATO', www.nato.int, 14 June 2022.

[86] 'NATO Strategic Concept 2022 ', 29 June 2022.

[87] Ibid, page 1.

[88] Ibid, paragraph 20-46.

[89] 'Wales Summit Declaration' 05 Sep. 2014.

[90] 'Brussels Summit Communiqué', 14 Jun. 2021.

[91] The Official NATO Terminology Database, https://nso.nato.int/natoterm/Web.mvc.

[92] 'The consultation process and Article 4', www.nato.int.

[93] Beside these meetings the NAC can meet at minister of defence, minister of Foreign affairs or Heads of State and Government level. The last ones would be the so-called NATO Summits.

National Military Representatives.[94] Information on malicious cyber activities or attacks could be exchanged at these forums but there is no obligation to report to NATO.

For the exchange of technical information on malicious cyber activities or attacks, NATO has other platforms. The NATO Information and Communication Agency (NCIA) Cyber Security Centre 'acts as a hub for real-time cyber information sharing, training and expertise for Allies and Partner Nations. Through our new Cyber Security Collaboration Network, National Computer Emergency Response Teams are able to quickly and securely share technical information with us and each other'.[95] This would be a better way to counter malicious cyber activities and attacks than officially or informally starting consultations to invoke NATO's crisis management process, as speed is of the utmost importance.

The NATO crisis management process (see Figure 3) starts with indications and warnings 'given either by NATO's intelligence and warning system or by an Ally or a partner. With these, there are in theory four options the Council can choose from: (i) decide that there is no need for further consideration; (ii) direct focused NATO vigilance and more information for the Council; (iii) consider diplomatic, political and precautionary responses, including civil emergency response and take into account military implications as appropriate; or (iv) decide to initiate a full assessment of the crisis situation'[96] and move to next phases. The military and political estimate (Phase 2) process involves the Strategic Command[97] and MC. Based on the response options developed by the Allied Command Operations (ACO) led by the Supreme Allied Commander Europe (SACEUR) and the advice of the MC, the NAC can decide to plan (Phase 4) and execute (Phase 5) an operation. During execution, Periodic Mission Reviews will allow the NAC to assess progress towards the desired end state. These reviews provide recommendations by the SC for changes to be considered by the MC and the NAC. When the desired mission end state is reached 'NATO moves into Phase 6 transition and, if needed, plans and implements a handover to the appropriate authorities, completes the military mission and progressively withdraws NATO forces'.[98] As shown in Figure 3, the NAC will make a consensus-based decision in every phase, based on the developed plans and advice of the MC (also consensus-based), something that will take time with 31 nations.

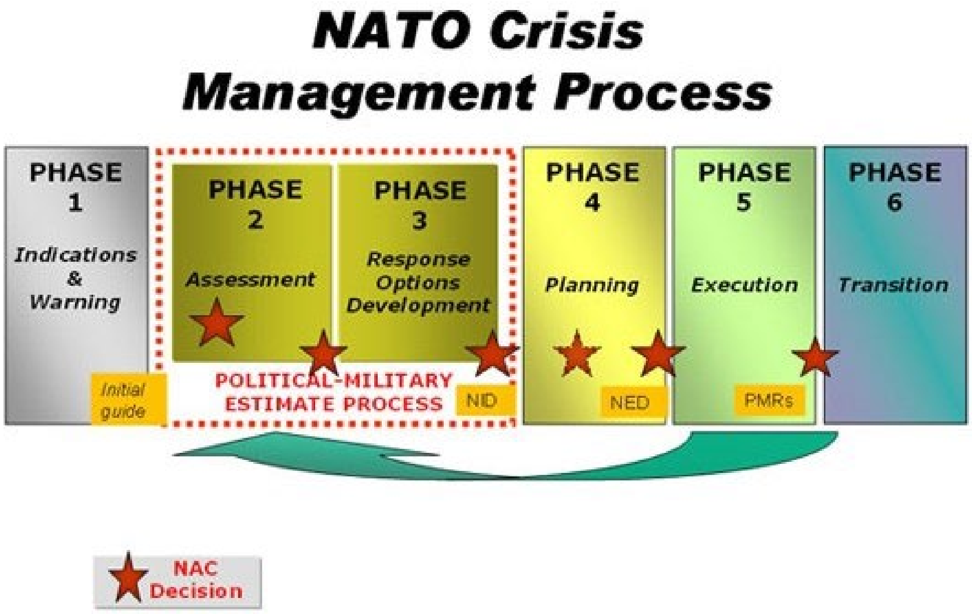


Figure 3. NATO crisis management process

[94] The MC meets also three times a year at the level of Chiefs of Defence.

[95] 'NATO's Cyber Security Centre', www.NCIA.nato.int.

[96] 'NATO's assessment of a crisis and development of response strategies', www.nato.int.

[97] Strategic Commands are Allied Command Operations and Allied Command Transformation.

[98] 'NATO's assessment of a crisis and development of response strategies.

In 2021 NATO Allies reaffirmed that a ‘decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the NAC on a case-by-case basis. Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack’.[99] In a crisis, a member nation could ask for Article 4 discussions. Looking at the North Atlantic Treaty and the NATO crisis management process it is clear that there is no obligation for a NATO member nation to report to or involve NATO when a malicious cyber activity or attack constitutes a crisis. However, if such a situation occurs it is unlikely that a member nation would not inform NATO or ask for consultations.

[99] Brussels Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 14 June 2021.

6. The EU and crisis management

To describe how the EU would act on malicious cyber operations and attacks that constitute a crisis, we have to look at the EU definition of a crisis within the cybersecurity realm.

The NIS2 directive describes 'measures for a high common level of cybersecurity across the Union'[100] but does not define a crisis; only a definition of a 'large-scale cybersecurity incident'[101] is given. The NIS2 directive refers to the Commission Recommendation (EU) 2017/1584[102] which states that 'a cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned member state to handle on its own or when it affects two or more member states with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level'.

Article 23 of the NIS2 directive describes the reporting obligations of member states, which shall ensure that 'essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority […] any incident that has a significant impact on the provision of their services'. [103] Essential or important entities are defined in Article 3 of the Directive and examples are given in the annexes.[104] An incident is considered significant if 'it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity [… or] has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage'.[105] These incidents first have to be reported to the national CSIRT without undue delay[106] and:

> 'and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;' [107] [… and] 'an incident notification, which, where applicable, shall update the information referred to in' the early warning [emphasis added] 'and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise'.[108]

As for informing other states and ENISA, Article 23 states that this has to be done where appropriate and without undue delay when the significant incident concerns two or more member states[109] through single points of contact that exercise a liaison function to ensure cross-border cooperation.[110] The NIS2 Directive tasks the member states to adopt a National Cyber Security Strategy including relevant procedures for appropriate information-sharing tools.[111] The Commission Recommendation gives a 'Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises'[112] that can be used for integration into existing EU crisis management mechanisms.

When the scale and effect of the malicious cyber activity or attack would rise to the level of an armed attack a state may exercise its inherent right of self-defence. For the EU this would mean the invocation of the mutual defence clause,

[100] NIS2 Directive.

[101] NIS2 Directive, Article 6, paragraph 1(7), 'large-scale cybersecurity incident' means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.

[102] Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises, 13 September 2017.

[103] NIS2 Directive, Article 23 paragraph 1.

[104] Ibid, Annex I and Annex II. Examples are entities in the energy, banking, financial markets health, drinking water sector.

[105] Ibid, Article 23 paragraph 3.

[106] Note that the NIS2 uses 'CSIRT or, where applicable, its competent authority' but for readability the term CSIRT is used in this Article.

[107] NIS2 Directive, Article 23 paragraph 4.a.

[108] Ibid, Article 23 paragraph 4.b.

[109] Ibid, Article 23 paragraph 6.

[110] Ibid Article 8.

[111] Ibid Article 7.

[112] Commission Recommendation (5).

Article 42.7 [113] of the Treaty on the Functioning of the European Union (TFEU). The solidarity clause of the TFEU, Article 222, states that ‘the Union and its member states shall act jointly in a spirit of solidarity if a member state is the object of a terrorist attack or the victim of a natural or man-made disaster’. Malicious cyber activity or an attack could be terrorist attacks or create a man-made disaster. Both create a situation where a state can ask for support. As for Article 222, there is no clear obligation to report and it would be for the state to decide whether it would make such a request.

Malicious cyber operations and attacks are cybersecurity incidents, the term used in EU legislation. When the disruption caused reaches a level that it becomes too extensive to handle for a single member state or when two or more member states are affected with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at the EU political level,[114] the incident has to be reported.[115]

[113] Treaty on the Functioning of the European Union:

> If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.

[114] Ibid, introduction (2).

[115] NIS2, Article 23 paragraph 6.

7. Summary

The analyses looked at the OED, literature and Estonian legislation definition of a crisis. Based on these sources, a crisis would at least have two elements: an event or chain of events that cause danger or threats and the need for urgent or prompt actions to deal with it. Using the groups of threats detailed in the ENISA 2022 report, it can be concluded that there is an overlap in the described threats that could cause the chain of events. Based on the five groups of harms described in the 'Taxonomy of cyber-harms', it is not the threat but rather the effect caused when the threat materialises that is decisive for the conclusion of whether it constitutes a crisis. There must be a certain level of harm to decide whether a malicious cyber event or attack constitutes a crisis. As there is no general rule on what level of harm constitutes a crisis, a decision has to be taken on a case-by-case basis.

When a cyber operation reaches the level of an armed attack and a state exercises its inherent right of self-defence under Article 51 of the UN Charter, this should immediately be reported to the Security Council. In other situations where a nation does not have the capacity to respond to a sudden-onset crisis or substantial deterioration of a humanitarian situation triggered by natural and human-induced hazards or conflict, it can request UN support. The criteria could be scale, complexity, urgency, capacity and risk of failure to deliver [humanitarian assistance] at large scale to affected populations. It is a national prerogative to decide to report to the UN and ask for assistance and such a decision would have to be made on a case-by-case basis.

For NATO, in 2021 the NATO Allies reaffirmed that a 'decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the NAC on a case-by-case basis. Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack'.[116] For a crisis, a member nation could ask for Article 4 discussions. Looking at the North Atlantic Treaty and the NATO crisis management process, it is clear that there is no obligation for a NATO member nation to report to or involve NATO, when a malicious cyber activity or attack constitutes a crisis. However, if such a situation occurs it is unlikely that a member nation would not inform NATO or ask for consultations.

In the EU, the legislation uses the term 'cybersecurity incidents' and these cover malicious cyber operations and attacks. When the disruption caused reaches a level that is too extensive to handle for a single member state or when two or more member states are affected with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at the Union political level, the incident has to be reported. Besides this reporting mechanism, a state can request support under Article 222 of the TFEU. The flowchart in Annex A can be used to determine if an incident has to be reported and to whom. Annex B contains a flowchart that can be used to define a response to a malicious cyber activity or attack.

A decision to report malicious cyber activities or attacks or to take action on them would depend on more than just legal factors.

[116] Brussels Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 14 June 2021

Abbreviations

ACO	Allied Command Operations
BGP	Border Gateway Protocol
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CNI	Critical national infrastructure
DDoS	Distributed denial-of-service
FED	Federal Reserve System
EU	European Union
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
OEWG	Open-Ended Working Group
MC	Military Committee
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NCIA	NATO Information and Communication Agency
OED	Oxford English Dictionary
PoC	Point of Contact
IASC	Inter-Agency Standing Committee
ICT	Information and communications technologies
OCHA	Office for the Coordination of Humanitarian Affairs
RDoS	Ransom Denial-of-Service
SACEUR	Supreme Allied Commander Europe
SCADA	Supervisory control and data acquisition
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
UNISDR	International Strategy for Disaster Reduction
US	United States

ANNEX A Reporting Mechanism

1. Note that the EU regulations speak of cybersecurity incident

2. Article 42(7) of the Treaty on European Union (TEU), legal threshold: an (I) armed aggression (II) on the territory of a Member State. Armed attack as described in the North Atlantic Treaty is pending on scale and effect.

3. **article 222**:
The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

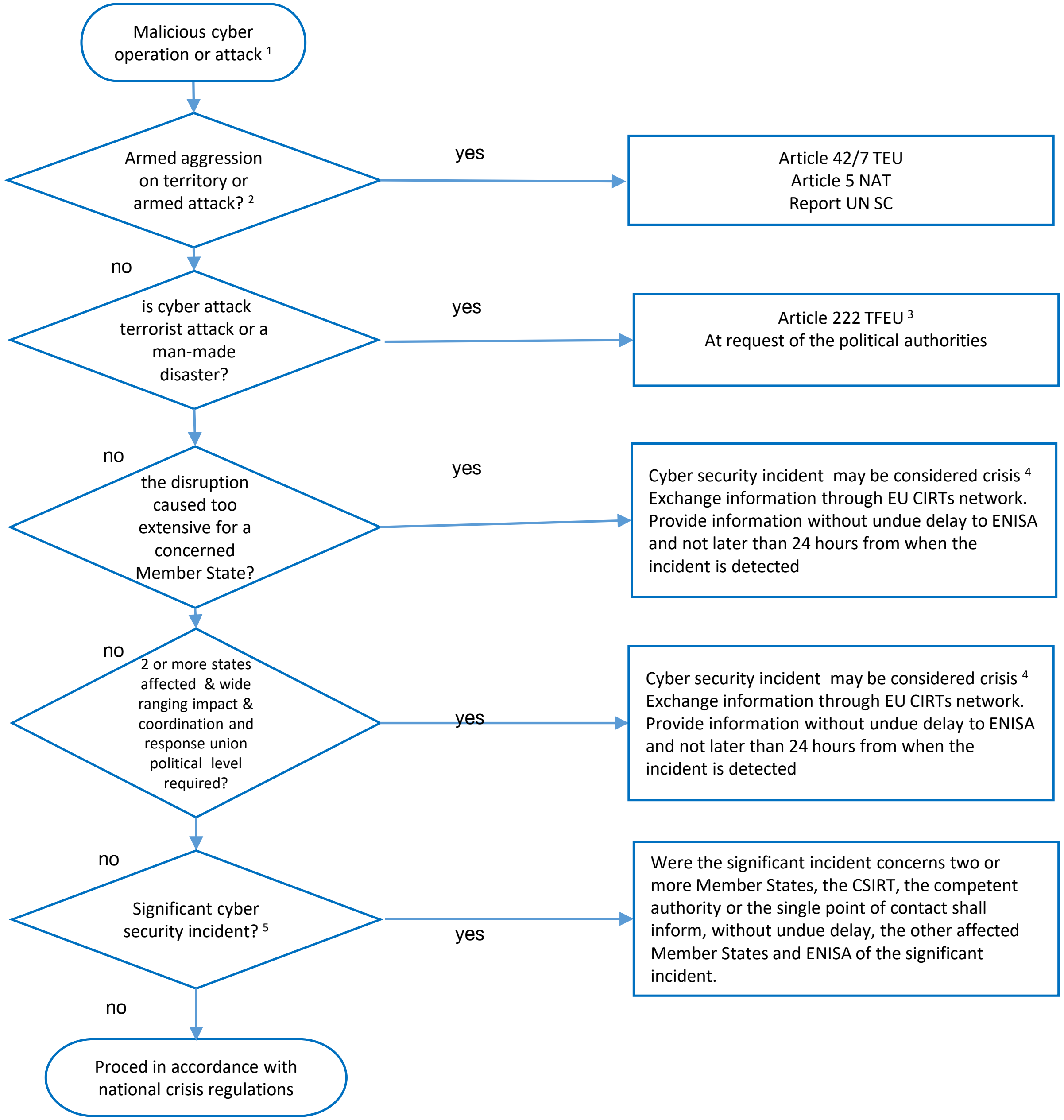
(a)
— prevent the terrorist threat in the territory of the Member States;
— protect democratic institutions and the civilian population from any terrorist attack;
— assist a Member State in its territory**, at the request of its political authorities**, in the event of a terrorist attack;

(b) assist a Member State in its territory, **at the request of its political authorities**, in the event of a natural or man-made disaster.

2. Should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

4 A cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned Member State to handle on its own
or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level

5 An incident shall be considered to be significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material
Damage



Malicious cyber operation or attack [1]

Armed aggression on territory or armed attack? [2]

yes

Article 42/7 TEU
Article 5 NAT
Report UN SC

no

is cyber attack terrorist attack or a man-made disaster?

yes

Article 222 TFEU [3]
At request of the political authorities

no

the disruption caused too extensive for a concerned Member State?

yes

Cyber security incident may be considered crisis [4]
Exchange information through EU CIRTs network.
Provide information without undue delay to ENISA and not later than 24 hours from when the incident is detected

no

2 or more states affected & wide ranging impact & coordination and response union political level required?

yes

Cyber security incident may be considered crisis [4]
Exchange information through EU CIRTs network.
Provide information without undue delay to ENISA and not later than 24 hours from when the incident is detected

no

Significant cyber security incident? [5]

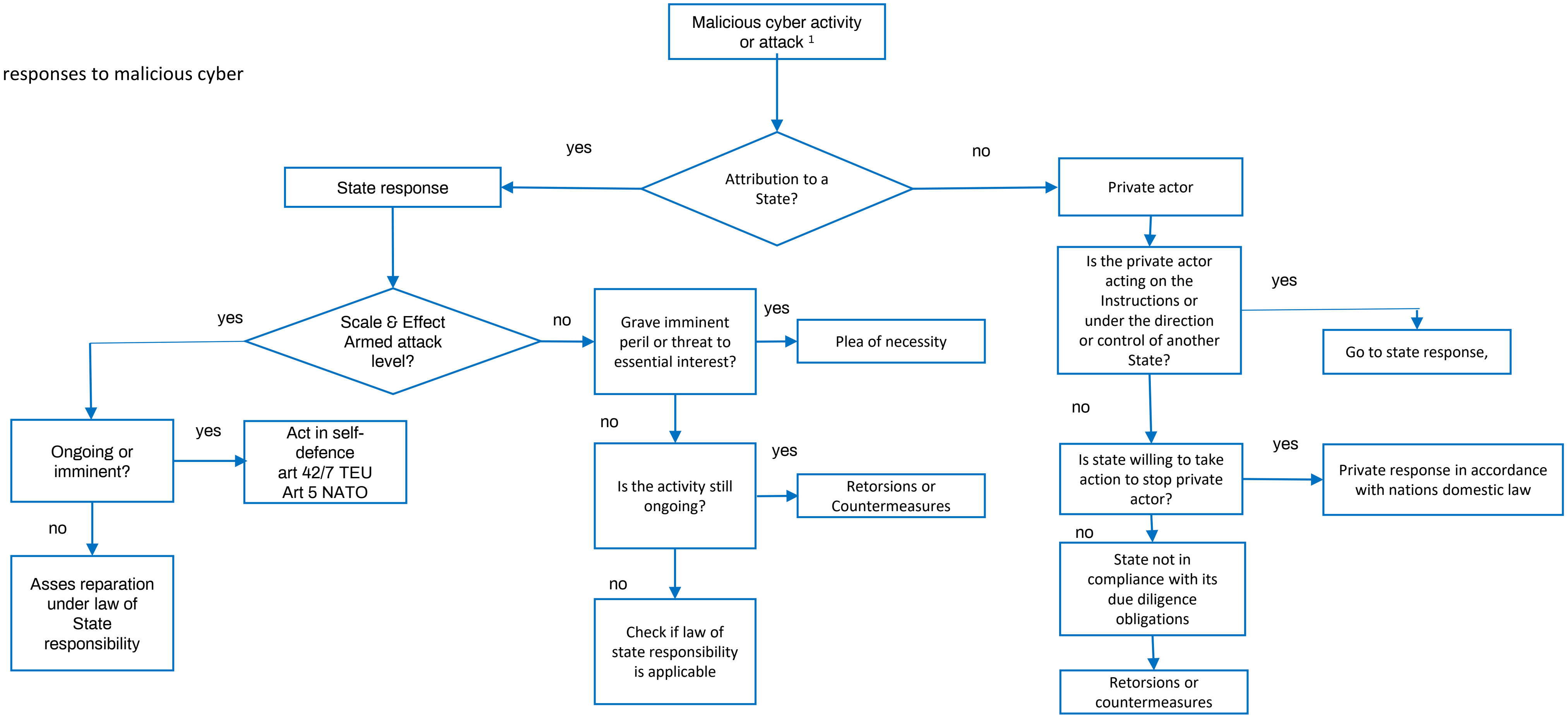
yes

Were the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident.

no

Proced in accordance with national crisis regulations

Annex B Flowchart responses to malicious cyber activity or attack



Malicious cyber activity or attack [1]

Attribution to a State?

yes

State response

Scale & Effect Armed attack level?

yes

Ongoing or imminent?

yes

Act in self-defence art 42/7 TEU Art 5 NATO

no

Asses reparation under law of State responsibility

no

Grave imminent peril or threat to essential interest?

yes

Plea of necessity

no

Is the activity still ongoing?

yes

Retorsions or Countermeasures

no

Check if law of state responsibility is applicable

no

Private actor

Is the private actor acting on the Instructions or under the direction or control of another State?

yes

Go to state response,

no

Is state willing to take action to stop private actor?

yes

Private response in accordance with nations domestic law

no

State not in compliance with its due diligence obligations

Retorsions or countermeasures

1 This flowchart is just a practical tool to assist Legal Advisors finding response option to a malicious cyber activity or attack. When deciding on response options all aspects of the malicious cyber activity or attack should be taken into account

2 The scale and effect of a malicious cyber activity or attack would lead to the decision whether it reaches the level of an armed attack

References

- https://un.mfa.ee/estonia-in-the-security-council-the-first-year/ 'Informal meeting on cyberstability and conflict prevention'
- ENSIA Threat Landscape, European Union Agency for Cybersecurity, 2022
- A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese and David Upton, Journal of Cybersecurity, 16 October 2018
- Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021
- Open-ended working group on developments in the field of information and telecommunications in the context of international security, A/AC.290/2021/CRP.2, 10 March 2021
- Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), May 2009
- Crises and Crisis Management: Toward Comprehensive Government Decision Making 277, Uriel Rosenthal and Alexander Kouzmin, J-PART
- Estonian Emergency Act, passed 08.02.2017.
- A Murderous Cyber-Attack Is Only A Matter Of Time, Shashank Joshi (2020), The Economist, 17 November 2020; Global Water Intelligence (2021)
- Mekorot Continues Efforts To Secure Its Critical Infrastructure Against Cyber-Attacks, 1 July 25021
- Florida Water Treatment Plant Hit With Cyber Attack, Steve Kardon, Industrial Defender, 9 February 2021.
- Hackers Breach U.S. Marshals System With Sensitive Personal Data, New York Times, 27 February 2023 https://www.nytimes.com/2023/02/27/us/politics/us-marshals-ransomware-hack.html
- A Genocide Incited on Facebook, With Posts From Myanmar's Military, New York Times, 15 October 2018
- Myanmar: The social atrocity: Meta and the right to remedy for the Rohingya, Amnesty International, 29 September 2022
- Facebook asked to clarify role in fuelling 'Rohingya genocide', Phnom Penh Post, Mar 9, 2022
- Tallin Manual 2.0, Cambridge University Press, 2020
- Shipping company Maersk says June cyberattack could cost it up to $300 million, CNBN, 16 August 2012.
- 'The Maersk cyber attack - how malware can hit companies of all sizes', Hilary Walton, 11 September 2022
- "Chernobyl's radiation monitoring system has been hit by the worldwide cyber attack", The Independent, 27 June 2017
- Colonial Pipeline ransomware attack, Wikipedia
- 'Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack', Vanessa Romo, NPR, 11 May 2021
- 'Carr: Kemp Declares State of Emergency due to Colonial Pipeline Cyber Incident, Invokes Price Gouging Statute', Office of the Attorney-General of the State of Georgia, 11 May 2021
- 84 JBE 2021 State of Emergency - Colonial Pipeline.pdf ' proclamation number JBE 2021-84', State of Louisiana (12 May 2021)
- 'Executive Order No. 213', State of North Carolina, 10 May 2021
- 'Executive Order Number Seventy-Eight (2021)', Office of the Governor of the Commonwealth of Virginia 11 May 2021
- 'Cyberattacks, Psychological Distress and Military Escalation': An Internal Meta-Analysis, Ryan Shandler, Michael L Gross, Daphna Canetti, Journal of Global Security Studies, Volume 8, Issue 1, March 2023.
- 'Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack'. Politico, 5 October 2022.
- Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania, White House, 07 September 2022

- Implications of Cyber Risk for Financial Stability, FED, 12 May 2022
- Hackers Breach U.S. Marshals System With Sensitive Personal Data', New York Times, 27 February 2023
- Misinformation on COVID-19: what did we learn?', EU knowledge hub, 21 February 202,
- Election misinformation helped fuel the Jan. 6 Capitol attack. Now, climate misinformation threatens the planet', Washington Post, 6 January 2022.
- Facebook Hosted Surge of Misinformation and Insurrection Threats in Months Leading Up to Jan. 6 Attack, Craig Silverman ProPublica, Craig Timberg The Washington Post, Jeff Kao ProPublica and Jeremy B. Merrill, The Washington Post, 4 January 2022
- Humanitarian System-Wide Scale-Up Activation Protocol 1: Definition and Procedures, endorsed by Endorsed by IASC Principals, November 2018, https://interagencystandingcommittee.org/iasc-transformative-agenda/content/iasc-protocol-1-humanitarian-system-wide-scale-activation
- Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats', UN OCHA, 2022.
- The North Atlantic Treaty, Washington D.C., 4 April 1949.
- NATO Checklist, www.nato.int.
- What is NATO? www.nato.int.
- 'Consensus decision-making at NATO', www.nato.int, 14 June 2022.
- NATO Strategic Concept 2022, 29 June 2022.
- Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 Sep. 2014.
- Brussels Summit Communiqué', Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 14 June 2021.
- The Official NATO Terminology Database, https://nso.nato.int/natoterm/Web.mvc.
- The consultation process and Article 4', www.nato.int.
- NATO's Cyber Security Centre, www.NCIA.nato.int
- NATO's assessment of a crisis and development of response strategies, www.nato.int
- DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 14 December 2022.
- Commission Recommendation (EU) 2017/1584 on a coordinated response to large-scale cybersecurity incidents and crises, 13 September 2017.
- Treaty on the Functioning of the European Union, Official Journal of the European Union, 26 October 2012.