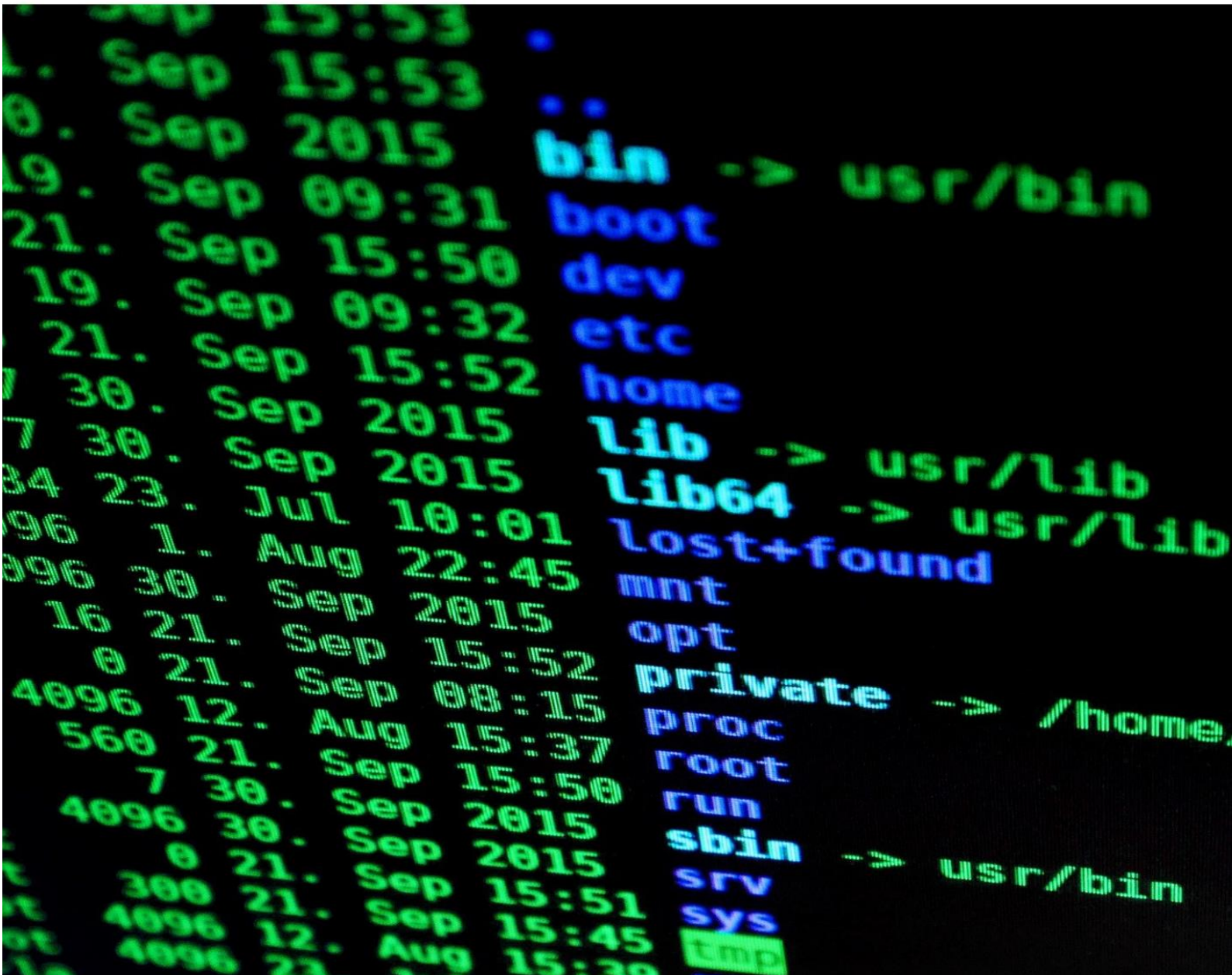
BACKGROUND PAPER

UN SECURITY COUNCIL:
OVERCOMING THE THREAT OF CYBER-ATTACKS TO KEY STATE INFRASTRUCTURE



1. Welcome Letter

Dear Delegates,

We are happy to welcome you to the Security Council at GrunnMUN 2022. The Security Council is arguably the most powerful UN organ as it can impose real binding obligations upon member countries. The Security Council is conferred with the "primary responsibility for the maintenance of international peace and securit**y**".[1] As you are aware, fifteen countries are represented in the Council. The five permanent members United States of America, Russia, France, China and the United Kingdom each have a veto. The other ten spots are alternated between the other UN members every two years. Which countries are represented, is voted upon by the General Assembly.[2] In order for a resolution to pass, there must be no veto and at least nine votes in favour.[3] Like all countries, permanent members who do not completely agree, but do not want to veto, may abstain as well.[4] Besides the permanent members, the following countries will be represented: India, North Korea, Estonia, Ethiopia, Germany, Saudi Arabia, Israel, Iran, Australia and Ukraine.

Let us briefly introduce ourselves:

Yara Lilie de Leon

Hi, I'm Yara, 21 years old, and a first-year bachelor's student at the University of Groningen, studying Communications and Information and passionate MUN-person. I first got involved in MUN in 2017 at a local conference in Zurich, Switzerland, and have gone down the rabbit hole of attending conferences ever since. I have been a delegate, have chaired and been on the organising team of countless MUNs. This, however, will be my first conference in the Netherlands, and I am very much looking forward to chairing the Security Council together with Emma. Besides MUNs and university, I am a bartender at a Club in Groningen, a stylist for a Dutch jeans brand and a passionate reader of young adult books.

Emma Lehbib

Hello lovely delegates, my name is Emma, I am 19 years old and I study International and European Law at RUG. Just like Yara, my passion for political simulation sparked in 2017 at my school's MUN. That continued when being in various positions at several MUN and Model European Parliament conferences in the following years. During my political simulation journey, I had the pleasure of travelling to different European cities. When I am not at the library or a conference, I enjoy spending time with friends and family, being active for the Sahrawi cause or practicing a new language. Now I

[1] UN Charter Art. 24 (1).
[2] UN Charter Art. 23 (1).
[3] United Nations, 'Voting System' *UN*, https://www.un.org/securitycouncil/content/voting-system (accessed 11 January 2022).
[4] ibid.

am happy to chair the Security Council together with Yara at GrunnMUN 2022.

The following background paper will provide you with relevant information on O*vercoming the Threat of Cyber-Attacks on Key State Infrastructure*. Yet, the preparation starts after reading this paper. Then it is on you to inform yourself on the position of the country you are representing and find possible answers to the afore-mentioned question. In case you have questions do not hesitate to contact us.

We are very much looking forward to a productive and enlightening session with you.

Yours sincerely,

Yara and Emma
(yara.lilie@gmail.com, emmalehbib1403@gmail.com)

The Chairs of the Security Council
GrunnMUN 2022

2. Introduction

At GrunnMUN 2022, the Security Council will be dealing with:

"Overcoming the Threat of Cyber-Attacks to Key State Infrastructure."

Yet, the preparation starts after reading this paper. Then, it is on you to inform yourself on the position of the country you are representing and find possible answers to the afore-mentioned question.

Although the digital world has provided us with an abundance of opportunities, digitalisation confronts States and their citizens with unprecedented challenges and dangers – one of them being cyberwarfare.

Cyberwarfare is defined as a cyber-attack or sequence of cyber-attacks on a State,[5] and has been developing into an alarmingly common practice. The headlines on cyber-attacks have been accumulating the past years as countries have been increasingly relying on digitalisation. Moreover, investigations on cyber-attacks shed light on possible links between cyber attacks and States. Governments are developing cyberwarfare strategies to pursue their political agendas.

How real and close to home this threat is, has become clear at latest after evidence of Global surveillance practices were leaked by Whistle-blower Edward Snowden in 2013.

Mayor cyber-attacks on key infrastructure can seriously impact a country and its people. Examples of targets can be hospitals, oil pipelines, food chains, health care system as well as government administration.[6]

The shift to non-traditional forms of warfare means States have to develop new ways of protection. In the Security Council, we debate possible approaches to overcome and prevent those attacks to countries' key infrastructure.

[5] 'What is Cyber Warfare' *Imperva*, https://www.imperva.com/learn/application-security/cyber-warfare/, (accessed 11 January 2022).

[6] Stamford, 'Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans', 2021, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we, (accessed 11 January 2022).

3. Problem specification

With the growing cyber dependency, the problem of the threat of cyber-attacks to key State infrastructure is very real and imminent. The implications can be grave: physical damage, costs of damage and even human lives are at stake.

Cyber-attacks can be responsible for physical damage. In 2014, a German plant's network was hacked. According to the German Federal Office for Information Security, cyber predators gained access to logins of mill's control systems, the plant failed and the blast furnace could not be shut down timely. This led to "massive damage".[7] Previously, the Iranian nuclear program was targeted by malicious Stuxnet worm.[8] Supposedly, almost 1000 centrifuges were destroyed by the attack in 2010.[9] As digital rights activist Benjamin Sonntag commented: ""We do not expect a nuclear power plant or steel plant to be connected to the internet. To be computerised, but to be connected to the internet and to be hackable - that is quite unexpected".[10] Hence, a connected issue with cyber-attacks is that vulnerability of infrastructure is rather identified after an (attempted) attack.

Logically, physical damage equals economic and financial loss. Being the target of cyberwarfare is costly. For example, the Australian Cyber Security Growth Network estimates that cyber-attacks may cause the loss of 30 billion Australian dollars to the domestic economy – roughly 1.5% of the Australian GDP – and displace more than 150 000 jobs.[11] In the past years, defence and military budgets of various states include spendings on the protection against and development of their very own cyberattacks.

Moreover, there is a human cost to cyberwar. The International Committee of the Red Cross provided a comprehensive report warning about the human costs of cyberwarfare as the delivery of essential services such as electrical grids or health care sector may be impacted.[12] In light of the pandemic, an attack on a hospital will have detrimental effects on the patients, possibly leading to long-term

[7] 'Hack attack causes 'massive damage' at steel work, *BBC*, 2014, https://www.bbc.com/news/technology-30575104, (accessed 11 January 2022).
[8] Brent Kesler, 'The Vulnerability of Nuclear Facilities to Cyber Attack', 2011, p. 15. http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf, (accessed 11 January 2022).
[9] William J. Broad, John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iranian Nuclear Delay". *New York Times*, January 15, 2011.
[10] 'Hack attack causes 'massive damage' at steel work, *BBC*, 2014, https://www.bbc.com/news/technology-30575104, (accessed 11 January 2022).
[11] 'We would lose $30 billion in weeks from cyberwar. But the real loss is the erosion of public trust', *UNWS Sydney*, 2020 https://www.unsw.edu.au/news/2020/07/we-could-lose--30-billion-in-weeks-from-cyberwar--but-the-real-l, (accessed 11 January 2022).
[12] ICRC, 'The potential human cost of cyber operations', *International Committee of the Red Cross*, 2019, https://www.icrc.org/en/document/potential-human-cost-cyber-operations, (accessed 11 January 2022); 'The Human Cost of Cyberwar', *Cyber Security Intelligence*, https://www.cybersecurityintelligence.com/blog/the-human-cost-of-cyberwar-4357.html, (accessed 11 January 2022).

consequences or even death.[13] In a Research paper, Susan W. Bremmer and Leo L. Clarke explore the role of civilians in cyber warfare and identify five possible ways of suffering a casualty.

- Civilians could be directly targeted;
- Civilians can be means to attack others;
- Civilians could be targeted indirectly;
- Casualty can be suffered during a counter response of the very own government; and
- The civilian is a combatant.[14]

It is important to note, there are cyber operations during armed conflicts. As we can tell, cyber-attacks are used supplementary to foreign policies and military strategies by states to pursue their respective political agendas.

Another challenge is that, different from traditional forms of warfare, there is a considerably lower threshold to launch cyber-attacks. Access to the internet and a computer can be sufficient to have a serious impact. Furthermore, cyber predators can pursue their practices remotely – there are no geographical limits.

Responsible and relevant actors are firstly, the States themselves and secondly, agencies. On the UN level, it is the UN Office of Counter-Terrorism (UNOCT).[15]

In light of the GrunnMUN 2022 theme, "Moving Forward: Fostering Development in a Globalised World", it is incredibly important to tackle the threat of cyber-attacks to key State infrastructure in order to sustain already achieved developments and safely improve on them.

[13] Laurent Gisel, Tilman Rodenhäuser and Kubo Mačák, 'Cyber-attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?' https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/, (accessed 11 January 2022).
[14] Susan W. Brenner and Leo L. Clarke, Civilians in Cyberwarfare: Casualties, 2010, https://www.researchgate.net/publication/45402471_Civilians_in_Cyberwarfare_Casualties, (accessed 11 January 2022).
[15] Cybersecurity, *United Nations Office of Counter-Terrorism,* https://www.un.org/counterterrorism/cybersecurity, (accessed 11 January 2022).

4. Questions a Resolution Must Answer (QARMA's)

We hope that the QARMA sections for the GrunnMUN 2022 debate of the Security Council provide you with interesting new facts and helpful insights. Please note that these are questions that the resolution is intended to answer, hence you must investigate how your country stands on these questions. If you have further ideas on our Council topic that you would like to discuss, please do not hesitate to address them in the debates as well.

1) Due to its rapid development, cyberspace is relatively young and unregulated. Therefore, it is important to define and differentiate between 'cyberwarfare' and 'cyber-attacks' in the context of international law to create legal certainty.

2) What specific measures can be taken to prevent attacks on critical infrastructure?

3) How could an international framework be established to increase international cybersecurity?

5. Explanatory Section Per QARMA

5.1. QARMA 1: Due to its rapid development, cyberspace is relatively young and unregulated. Therefore, it is important to define and differentiate between 'cyberwarfare' and 'cyber-attacks' in the context of international law to create legal certainty.

5.1.1. History / Background of the Problem

The term *Cyberwar* was first coined in an Omni magazine issued 1987, however, in a very different context. It was used to give a futuristic description of how wars will be fought in the future: "giant robots, autonomous flying vehicles, and autonomous weapons systems".[16] That science-fiction turned out to be less spectacular – at least in respect to the required technological advancements. Cyberwarfare would just require computers and the internet. The RAND analysts John Arquilla and David Ronfeldt warn about military hacking being utilised to attack / disrupt enemies' computers.[17] Over the years, it became clear that there are other potential targets: key infrastructures which could have serious implications on the enemy and their civilians.[18] In their book 'Cyber War', Richard Clarke and Robert Knacke define cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption".[19] Yet, this is a rather limited definition, especially when keeping in mind how quickly and sophisticated cyber-tools have been developing during the past decade.

The era of Web War I arguably began almost fifteen years ago in Estonia.[20] Estonia is a heavily digitalised country and therefore, the probably most interesting and accessible prey for cyber-attacks. The unprecedented attack was sparked after a memorial to the Soviet Red Army was meant to be moved to a less prominent place. The announcement led to riots and lootings, and was soon followed by a series of cyber-attacks. Botnets spread vast amounts of spams and online requests to local banks, government institutions and media outlets. There is no clear evidence on who is responsible, only speculations.[21]

---

[16] Andy Greenberg, 'What Is Cyberwar? The Complete WIRED Guide', *WIRED*, https://www.wired.com/story/cyberwar-guide/, (accessed 11 January 2022).
[17] John Arquilla and David Ronfeldt, Cyberwar is Coming! *RAND Corporation* https://www.rand.org/pubs/reprints/RP223.html, (accessed 11 January 2022).
[18] Andy Greenberg, 'What Is Cyberwar? The Complete WIRED Guide', *WIRED*, https://www.wired.com/story/cyberwar-guide/, (accessed 11 January 2022).
[19] ibid.
[20] ibid.
[21] Damien McGuiness, 'How a cyber-attack transformed Estonia', *BBC*, 2017, https://www.bbc.com/news/39655415, (accessed 11 January 2022).

The year 2010 marks a turning point. The idea of cyberwar was heavily shaped, when Stuxnet – "the most sophisticated piece of code ever engineered for a cyberattack"[22] – was detected. As previously mentioned, it was created to demolish Iran's nuclear enrichment facilities' centrifuges. It was the NSA's and Israeli intelligence's attempt to hinder Iran's nuclear bomb plans.[23]

5.1.2. Recent Developments

This timeline encompasses just a few of the cyber incidents in the past years:

2012

Shamoon attack on Saudi Aramco[24]

2014

Sony Pictures Hack[27]

2015

Ukraine power grid hack[25]

June 2017

NotPetya[28]

August 2017

Triton (malware)[26]

In an interview with BBC, the IISS specialist on future warfare Franz-Stefan Gady warns that civilians will be more affected in future wars "because great powers are massively investing not only in offensive cyber capabilities but also in electronic warfare capabilities that can jam satellites and bring down communication. So not just the military but societies overall will be a prime target in future conflict".[29]

5.1.2.1. Types of Cyber Attacks

[22] Andy Greenberg, 'What Is Cyberwar? The Complete WIRED Guide', *WIRED*, https://www.wired.com/story/cyberwar-guide/, (accessed 11 January 2022).
[23] David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks against Iran, *The New York Times*, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html, (accessed 11 January 2022).
[24] Compromise of Saudi Aramco and RasGas, *Council on Foreign Relations*, 2012, https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas, (accessed 11 January 2022).
[25] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, *WIRED*, 2016 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, (accessed 11 January 2022).
[26] Matrin Giles, 'Triton is the world's most murderous malware, and it's spreading', *MIT Technology*, 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/, (accessed 11 January 2022).
[27] Emily Van Der Reff and Timothy B. Lee, 'The 2014 Sony hacks, explained', *Vox*, 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea, (accessed 11 January 2022).
[28] Josephine Wolff, 'How the NotPetya attack is reshaping cyber insurance', *Tech Stream*, 2021, https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/, (accessed 11 January 2022).
[29] Frank Gardner, 'What does future warfare look like? It's already here, *BBC*, https://www.bbc.com/news/world-59755100, (accessed 11 January 2022).

Source of Image: see Footnote 35

Espionage: "Is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity".[30]

Propaganda Attacks: "Disseminating false or misleading information to sway public opinion by way of social media, fake news websites and any other digital means".[31]

Denial-of-Service Attack (DoS): "Is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected".[32]

Sabotage: "Coordinating with computers' and satellites' vulnerable components to lead to disruption of systems via a distributed-denial-of-service (DDoS) attack".[33]

Electrical Power Grid: "Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable".[34]

Economic Disruption: "Causing large-scale disruptions to negatively affect a company or group of importance for a country".[35]

Surprise Attacks: "The non-traditional, asymmetric or irregular aspect of cyber action against a State".[36]

---

[30] 'What is Cyber Espionage', *vmware*, https://www.vmware.com/topics/glossary/content/cyber-espionage.html, (accessed 11 January 2022).
[31] Shanmugavel Sankaran, 'Is the World Ready for A Cyberwar', *Forbes*, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/08/30/is-the-world-ready-for-a-cyberwar-/?sh=4f59a5507b8, (accessed 11 January 2022).
[32] 'What is a denial of service (DoS)?', *Paloalto Networks*, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, (accessed 11 January 2022).
[33] Shanmugavel Sankaran, 'Is the World Ready for A Cyberwar', *Forbes*, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/08/30/is-the-world-ready-for-a-cyberwar-/?sh=4f59a5507b80, (accessed 11 January 2022).
[34] 'What is Cyber Warfare' *Imperva*, https://www.imperva.com/learn/application-security/cyber-warfare/, (accessed 11 January 2022).
[35] Shanmugavel Sankaran, 'Is the World Ready for A Cyberwar', *Forbes*, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/08/30/is-the-world-ready-for-a-cyberwar-/?sh=4f59a5507b8, (accessed 11 January 2022).
[36] ibid.

5.1.3. International Approaches That Have Already Been Undertaken

It is crucial to differentiate cyberwar from cybercrime. All cyber-attacks are cybercrimes, but not all cybercrimes are acts of war.[37] An important question is at what point can a cyber-attack be considered an act of war? How can cyberwar be defined? The opinions on this are diverse. For example, CSIS Senior Vice President and Director James Andrew Lewis argues the threshold for cyberwar should be high.[38] However, being lenient on cyber-attacks allows for harm being committed without liability. Logically, the question arises, what kind of counter-responses and forms of self-defence are proportional and legitimate to employ after suffering a cyberattack? These are just a few questions that arise with the question of definition of cyberwarfare, which you will have to find a common answer to create a higher level of legal certainty, less potential for conflicts and most importantly save human lives.

Of course, cyber activities are to some degree regulated by International Law. Peremptory Norms and International Humanitarian Law apply.[39] For example, weapons that do not discriminate are prohibited.[40] This closely ties in with Article 36 of the Additional Protocol (I) to the Geneva Convention, which states:

> *"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."*

The review of new weapons might fall back with the rapid advancements made in the development of technology; however, it should not be neglected.

As members of the Security Council, you are tasked to find answers to these crucial questions for the global security of today and tomorrow.

5.1.4. Relevant Actors / Institutions

[37] Tony Bradley, 'When Is a Cybercrime an Act of Cyberwar?', *PCWorld*, 2012, https://www.pcworld.com/article/468398/when_is_a_cybercrime_an_act_of_cyberwar_.html, (accessed 11 January 2022).
[38] James Andrew Lewis, 'Thresholds for Cyberwar', *Centre for Strategic & International Studies*, 2010, https://www.csis.org/analysis/thresholds-cyberwar, (accessed 11 January 2022).
[39] 'Cyber Warfare: does International Humanitarian Law apply?', *ICRC*, 2021, https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law, (accessed 11 January 2022).
[40] 'Rule 71. Weapons That Are by Nature Indiscriminate' *IHL Database*, https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule71, (accessed 11 January 2022).

The **UN Office of Information and Communication Technology (OICT)** is tasked with amplifying a secure and sustainable future with the help of innovation and technology.[41]

Besides several other initiatives, the **UN Office of Counter-Tourism** launched the *Cybersecurity and New Technologies programme* with goal of improving the protection of member states and private organisations against cyber-attacks of terrorist actors against key infrastructure. Further, the programme aims to reduce the impact and help recover systems after cyber-attacks.[42]

NATO is committed to improve cyber security.[43]

The European Union created the Cybersecurity Strategy of the European Union.[44]

5.2. QARMA 2: What specific measures can be taken to prevent attacks on critical infrastructure?

5.2.1 History / Background of the Problem

To undertake measures, it must first be understood what types of attacks are realistically happening in the world. Which infrastructure is being attacked and which countries are being affected? Below, you can see a timeline of attacks ranging from 2016 to 2018. Out of the 13 attacks that are listed here, 8 affected critical national infrastructures.

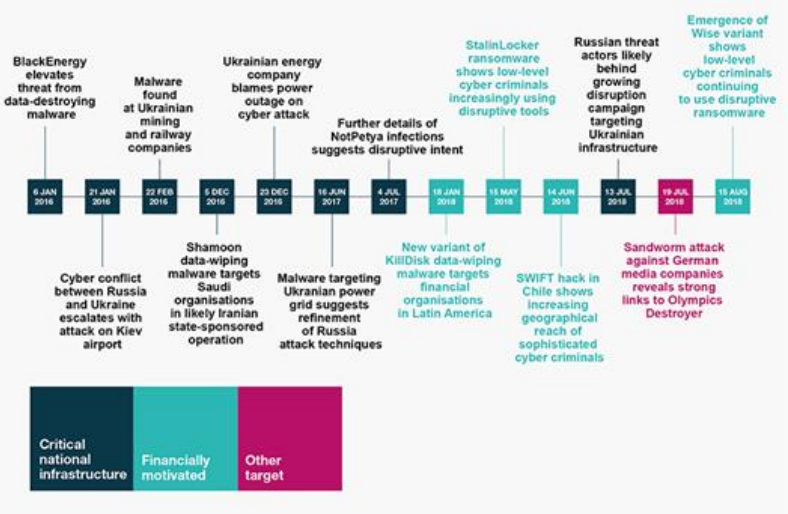


Image source[45]

[41] https://unite.un.org.
[42] https://www.un.org/counterterrorism/cybersecurity.
[43] https://www.nato.int/cyberdefence/.
[44] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.
[45] Vinugayathri Chinnasamy, Cyberwarfare: The new frontier of Wars between countries, https://www.infosecurity-magazine.com/blogs/cyberwarfare-frontier-wars/.

Critical Infrastructure (CII) is defined differently in the world. For Europe, critical infrastructure is made up of "electricity generation plants, transportation systems and manufacturing facilities".[46] While the USA takes a more general approach on the definition: CII "describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on their physical, economic security, public health or safety, their Nations critical infrastructure provides essential services that underpin the American society".[47] China's definition of CII is similar to both the EU's and the American definition, as China defines it as: "infrastructure from important industries and sectors, including public communication and information services, energy, transportation, water conservancy, finance, public service, and e-government, as well as other industries and sectors that may pose severe threat to national security, people's livelihood, and public interests if their data is damaged or disabled or leaked".[48]

Most of CII is controlled and monitored by Industrial Control Systems, such as the Supervisory Control and Data Acquisition systems also referred as SCADA. Most of the ICS products are nowadays based on standard embedded systems platforms, and therefore often use commercial off the shelf software. This, although cheaper and easier to use, increases the risk of exposure to computer network-based attacks.[49]

"Recent deliberate disruptions of critical automation systems prove that cyber-attacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social wellbeing. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level."[50]

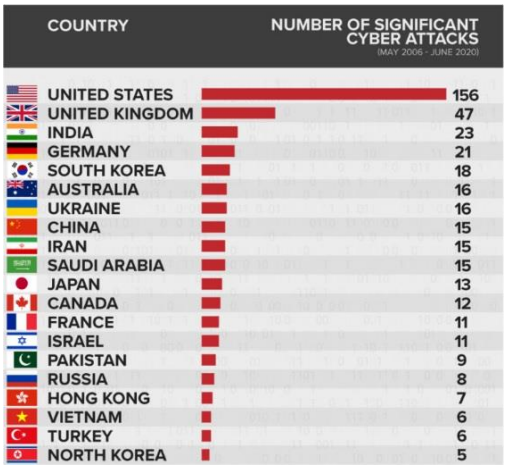
5.2.2. Recent Developments

As shown on the picture below, the number of significant cyber-attacks in the past 14 years is quite high. This is especially true for the United States and the United Kingdom.[51]

The severity of cyber-attacks and the occurrence of cyber-attacks have been growing at an alarming rate every year. The definition of a significant cyber-attack for this specific graphic is defined as: "cyber-attacks on a country's government agencies, defence and high-tech companies or economic

[46] ENISA, Critical infrastructures, and services, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.
[47] CISA, CISA's Role in Infrastructure security, https://www.cisa.gov/infrastructure-security.
[48] Latham & Watkins, China issues new regulations to protect the CII, https://www.lw.com/thoughtLeadership/China-Issues-New-Regulations-to-Protect-the-Critical-Information-Infrastructure#:~:text=Article%2031%20of%20the%20Network,industries%20and%20sectors%20that%20may.
[49] ENISA, Critical infrastructures and services, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.
[50] ENISA, Critical infrastructures and services, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.
[51] The evolving Enterprise, US is prey to 156 "significant" cyber-attacks since 2006 https://www.theee.ai/2020/07/20/3937-us-is-prey-to-156-significant-cyber-attacks-since-2006/.

crimes with losses equating to more than a million dollars. One of the most recent breaches that was aimed at the USA occurred in May of 2020 and found that Russian hackers where exploiting a bug that was commonly used in email servers, to infiltrate sensitive data from American organisations. One of the attacks that the UK fell prey to, was a large-scale cyber-attack that was deployed across the Labour Party's digital platforms during the elections in 2019.



These statistics, as well as the research behind the information, highlights the frequency of cyber-attacks which continuously affect key economic, social, and political institutions within different countries.[52]

5.2.3. Relevant Actors / Institutions

ENISA: One of the key players for the European Union is ENISA, which is the European Union Agency for Cybersecurity.

ECSO: The European Cybersecurity Organisation is another actor within the EU. It is a non-profit institution that was created in 2016.[53]

American Cybersecurity Institute: The ACI is a recent non-profit organisation that was formed to educate, advocate, study and analyse the space of cybersecurity law and policy.[54]

5.2.4. International Approaches That Have Already Been Undertaken

NIS Directive: Europe has come together at ENISA to create a directive on security of network and information systems (NIS Directive), in an attempt to collect data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) invest their budget on cybersecurity, and how this investment has been influenced by the NIS Directive.

The Directive represents one of the first EU-wide legislation on cybersecurity. The objective is to achieve a high common level of cybersecurity for all Member States.

[52] The evolving Enterprise, US is prey to 156 "significant" cyber-attacks since 2006 https://www.theee.ai/2020/07/20/3937-us-is-prey-to-156-significant-cyber-attacks-since-2006/.
[53] ECSO, European Cybersecurity Organisation, https://ecs-org.eu/
[54] Cybersecurity Intelligence, American Cybersecurity Institute, https://www.cybersecurityintelligence.com/american-cybersecurity-institute-5936.html.

5.3. QARMA 3: How could an international framework be established to increase international cybersecurity?

5.3.1. History / Background of the Problem

In order to establish a framework, it must first be understood what a framework means. In connection to cybersecurity, a framework is a summary or collection of guidelines and practices that ensure that the risk of being exposed to cyberattacks is reduced.

There are 5 main parts that a framework should entail. [55]

Identify: First you must understand which parts of your infrastructure are at risk and are possibly being exposed to a cyberattack. This gives you an idea of which parts need improvement.

Protect: You should take all possible measures to prevent an attack from happening in the first place, or to at least contain or limit the effect of an attack. To achieve this, corresponding safeguards must be developed and implemented. This could include physical security controls, firewalls, monitoring programs, education of employees etc.

Detect: A procedure should be put in place in order to easily and quickly identify breeches and attacks. An outline of the steps that should be taken once detected, should be established in order for the organisation to react quickly and in a controlled manner.

Respond: An incident response team should be put in place before it is needed and should have a clear step-by-step procedure for when an attack has been identified and until it is mitigated.

Recover: Once an attack has been mitigated, it is crucial to plan on recovery in order to restore crucial functions and services. A part of that recovery is also ensuring that the security issue is handled and fixed.[56]

5.3.2. Recent Developments

In March of 2021, the General Assembly, surprisingly unanimously agreed on a Cybersecurity report. The final report was created in the UN cybersecurity Open-Ended Working Group.

The paper contains recommendations for advancing peace and security within cyberspace. Although the report is not legally binding, it marks a development in the process of achieving agreement on international cybersecurity.

---

[55] Reciprocity, What is a Cybersecurity Framework, https://reciprocity.com/resources/what-is-a-cybersecurity-framework/.
[56] Reciprocity, What is a Cybersecurity Framework, https://reciprocity.com/resources/what-is-a-cybersecurity-framework/.

The paper lays out possible cooperative measures to address existing and potential threats in cyberspace. The measures include: "further development of rules, norms, and principles of responsible behaviour of States; how international law applies to the use of ICTs by States; confidence building measures; capacity building; and the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations".[57]

The agreement within the OEWG on this paper means that international security in cyberspace has become an issue that is discussed by all UN Member States.[58]

5.3.3. Relevant Actors / Institutions

OEWG: The open-ended working group is a crucial player in the cybersecurity discussion. Although their final report on cybersecurity was unanimously passed, and therefore concluded their work in 2021, another OEWG will begin its work in 2022.

The OEWG was established in December of 2018 by the General Assembly next to the Group of Governmental Experts. During their time, they focused on existing and emerging threats, how international law applies in the use of ICTs of States, Confidence and Capacity building measures.[59]

Group of Governmental Experts: Like the OEWG, the GGE was established by the General Assembly and was tasked on advancing responsible State behaviour in cyberspace in the context of international security.[60]

The GGE worked on their final report that contains the findings on existing and emerging threats; norms, rules and principles for the responsible behaviour of States; international law; confidence building measures; and international cooperation and assistance in ICT security and capacity building.[61]

5.3.4. International Approaches That Have Already Been Undertaken

Besides the Working Group and Group of Governmental Experts, the UN has established the Digital Blue Helmets (DHB) programme.

[57] OEWG, Working Paper United Nations, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
[58] Council on Foreign Relations, All UN countries agreed on a CS Report, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.
[59] United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/ict-security/.
[60] United Nations Office for Disarmament Affairs, Group of Governmental Experts, https://www.un.org/disarmament/group-of-governmental-experts/.
[61] UN GA GGE, Final Report, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

The DHB is intended to serve as a common platform for the exchange of information as well as the better coordination of protective and defensive measures against information technology security incidents for the UN, including programmes, agencies, and funds.[62]

[62] UN, The digital blue helmets, https://unite.un.org/digitalbluehelmets/.

6. Further Research

Center for Strategic & International Studies, Significant Cyber Incidents Since 2006: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104_Significant_Cyber_Events.pdf?dLSQUtb9qiFpttFl7FcBmA9IKZaNPUib.

Crowdstrike, Global Threat Report 2021: https://fbcinc.com/source/virtualhall_images/CyberMaryland/CrowdStrike/2021_Global_Threat_Report_FINAL_.pdf.

Cyber Warfare: Does International Humanitarian Law Apply?: https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.

ICRC Expert Meeting, The Potential Human Cost of Cyber Operation [14-16 November 2018, Geneva]: https://www.icrc.org/en/document/potential-human-cost-cyber-operations.

James A. Lewis, Thresholds for Cyberwar September 2010: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101001_ieee_insert.pdf.

Nils Melzer, Cyberwarfare and International Law [2 November 2011]: https://unidir.org/publication/cyberwarfare-and-international-law.

Ralph Langner, To Kill a Centrifuge I Detailed Stuxnet Analysis: https://www.langner.com/to-kill-a-centrifuge/#_Toc372371543.

Susan W. Brenner and Leo L. Clarke, Civilians in Cyberwarfare: Casualties July 2010: https://www.researchgate.net/publication/45402471_Civilians_in_Cyberwarfare_Casualties.

Tim Hsia and Jared Sperli, How Cyberwarfare and Drones Have Revolutionised Warfare: https://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/.

Vincent Boulanin and Maaike Verbruggen, ARTICLE 36 REVIEWS Dealing with the Challenges Posed by Emerging Technologies: https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf.

World Economic Forum, The Global Risks Report 2021: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

The General Assembly and Security Council have already passed several resolutions related to our question which you may look at:

- SC Resolution 64/211, 17 March 2010
- GA Resolution 58/199, 20 January 2004
- GA Resolution 57/239, 31 January 2003
- GA Resolution 56/121, 23 January 2002

7. Bibliography

Andy Greenberg, 'What Is Cyberwar? The Complete WIRED Guide', *WIRED,* https://www.wired.com/story/cyberwar-guide/, (accessed 11 January 2022).

Brent Kesler, 'The Vulnerability of Nuclear Facilities to Cyber Attack', 2011, p. 15, http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf, (accessed 11 January 2022).

CISA. (2020). *INFRASTRUCTURE SECURITY | CISA*. https://www.cisa.gov/infrastructure-security.

Chinnasamy, V. (2020, September 14). *Cyberwarfare: the New Frontier of Wars Between Countries*. Infosecurity Magazine. https://www.infosecurity-magazine.com/blogs/cyberwarfare-frontier-wars/.

Compromise of Saudi Aramco and RasGas, *Council on Foreign Relations,* 2012, https://www.cfr.org/cyber-operations/compromise-saudi-aramco-and-rasgas, (accessed 11 January 2022).

Cybersecurity, *United Nations Office of Counter-Terrrorism,* https://www.un.org/counterterrorism/cybersecurity, (accessed 11 January 2022).

'Cyber Warfare: does International Humanitarian Law apply?', *ICRC,* 2021, https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law, (accessed 11 January 2022).

Damien McGuiness, 'How a Cyber-attack Transformed Estonia', *BBC,* 2017, https://www.bbc.com/news/39655415, (accessed 11 January 2022).

David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks against Iran, *The New York Times*, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html, (accessed 11 January 2022).

Emily Van Der Reff and Timothy B. Lee, 'The 2014 Sony hacks, explained', *Vox,* 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea, (accessed 11 January 2022).

ENISA. (2020). *Critical Infrastructures and Services*. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services.

Frank Gardner, 'What Does Future Warfare Look Like? It's Already Here', *BBC,* https://www.bbc.com/news/world-59755100, (accessed 11 January 2022).

Group of Governmental Experts. (2021, July). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/135). United Nations. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

'Hack attack causes 'massive damage' at steel work, *BBC,* 2014, https://www.bbc.com/news/technology-30575104, (accessed 11 January 2022).

ICRC, 'The potential human cost of cyber operations', *International Committee of the Red Cross*, 2019, https://www.icrc.org/en/document/potential-human-cost-cyber-operations, (accessed 11 January 2022).

James Andrew Lewis, 'Thresholds for Cyberwar', *Centre for Strategic & International Studies*, 2010, https://www.csis.org/analysis/thresholds-cyberwar, (accessed 11 January 2022).

Josephine Wolff, 'How the NotPetya attack is reshaping cyber insurance', *Tech Stream*, 2021, https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/, (accessed 11 January 2022).

Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, *WIRED*, 2016 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, (accessed 11 January 2022).

Latham, & Watkins. (2021, September). *China Issues New Regulations to Protect the Critical Information Infrastructure* (No. 2892). Latham & Watkins. https://www.lw.com/thoughtLeadership/China-Issues-New-Regulations-to-Protect-the-Critical-Information-Infrastructure#:~:text=Article%2031%20of%20the%20Network,industries%20and%20sectors%20that%20may.

Laurent Gisel, Tilman Rodenhäuser and Kubo Mačák, 'Cyber-attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?' https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/, (accessed 11 January 2022).

Matrin Giles, 'Triton is the world's most murderous malware, and it's spreading', *MIT Technology,* 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/, (accessed 11 January 2022).

Ops, D. W. (2020, July 20). *US is prey to 156 'Significant' Cyber-attacks Since 2006*. The EE. https://www.theee.ai/2020/07/20/3937-us-is-prey-to-156-significant-cyber-attacks-since-2006/.

Politics, G. B. F. N. (2021, March 18). *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?* Council on Foreign Relations. https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

Reciprocity. (2021, August 11). *What Is a Cybersecurity Framework?* https://reciprocity.com/resources/what-is-a-cybersecurity-framework/.

'Rule 71. Weapons That Are by Nature Indiscriminate' *IHL Database,* https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule71, (accessed 11 January 2022).

Shanmugavel Sankaran, 'Is the World Ready For A Cyberwar', *Forbes,* 2021, https://www.forbes.com/sites/forbestechcouncil/2021/08/30/is-the-world-ready-for-a-cyberwar-/?sh=4f59a5507b8, (accessed 11 January 2022).

Stamford, 'Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans', 2021, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we, (accessed 11 January 2022).

Susan W. Brenner and Leo L. Clarke, Civilians in Cyberwarfare: Casualties, 2010, https://www.researchgate.net/publication/45402471_Civilians_in_Cyberwarfare_Casualties, (accessed 11 January 2022).

'The Human Cost of Cyberwar', *Cyber Security Intelligence,* https://www.cybersecurityintelligence.com/blog/the-human-cost-of-cyberwar-4357.html, (accessed 11 January 2022).

Tony Bradley, 'When Is a Cybercrime an Act of Cyberwar?', *PCWorld*, 2012, https://www.pcworld.com/article/468398/when_is_a_cybercrime_an_act_of_cyberwar_.html, (accessed 11 January 2022).

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, available at: https://www.refworld.org/docid/3ae6b3930.html (accessed 11 January 2022).

United Nations OEWG. (2021, March). *Final Substantive Report* (A/AC.290/2021/CRP.2). United Nations. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

UN Office for Disarmament Affairs. (2021). Developments in the field of information and telecommunications in the context of international security – UNODA. United Nations. https://www.un.org/disarmament/ict-security/.

UN Office for Disarmament Affairs. (2021b). *Group of Governmental Experts – UNODA*. United Nations. https://www.un.org/disarmament/group-of-governmental-experts/.

United Nations. (2017). *United Nations*. https://unite.un.org/digitalbluehelmets/.

United Nations, 'Voting System' *UN*, https://www.un.org/securitycouncil/content/voting-system (accessed 11 January 2022).

'We would lose $30 billion in weeks from cyberwar. But the real loss is the erosion of public trust', *UNWS Sydney*, 2020, https://www.unsw.edu.au/news/2020/07/we-could-lose--30-billion-in-weeks-from-cyberwar--but-the-real-l, (accessed 11 January 2022).

'What is a denial of service (DoS)?', *Paloalto Networks*, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, (accessed 11 January 2022).

'What is Cyber Espionage', *vmware*, https://www.vmware.com/topics/glossary/content/cyber-espionage.html, (accessed 11 January 2022).

'What is Cyber Warfare' *Imperva*, https://www.imperva.com/learn/application-security/cyber-warfare/, (accessed 11 January 2022).

William J. Broad, John Markoff, and David E. Sanger. “Israeli Test on Worm Called Crucial in Iranian Nuclear Delay”. *New York Times*, January 15, 2011.