Master Thesis – Department of International Affairs

TO WHAT EXTENT CAN CYBERATTACKS CONSTITUTE A GLOBAL CATASTROPHIC RISK?

An investigation into the nature, extent, and relevance of cyber-enabled global catastrophic risk.

Arthur Gustave Henri Duforest
Development and International Relations – Aalborg University

Table of Contents

Introduction 4
Methodology 5
Global Catastrophic Risk 7
Methodological considerations 8
Environmental Scanning 9
Quantifying impacts of leads on components - Numerical association 10
Classification of Global Catastrophic Risk 10
Critical system 10
Global spread mechanisms 11
Prevention, and mitigation failures 12
Theoretical Background 12
Benefit/Dependence/Risk theory 13
Cyber has its own rules. 14
Cyber security 15
Analysis 16
Public Sector Administrative Governance 16
Broad Governmental Vulnerability – The Case of Estonia 2007 18
Governmental Agency Vulnerabilities - The Solar Wind Hack 2020 20
Critical systems 21
Military systems 23
Digitalization of the Military – Offensive Cyber Capabilities 23
Military Applications of Cyber – NATO 26
Military Applications of Cyber – Russia 27
Military Vulnerabilities on the Field – The Ukrainian D-30 Howitzers 28
Military Applications of Cyber – Coordinated Military Intervention in Iran 2010 30
Military Vulnerability - The Theoretical Vulnerabilities of Nuclear Weapon Systems 31
Military Critical systems 32
Critical Infrastructure 33
Critical Infrastructure – Cyber-Physical System 33
Critical Infrastructure Interdependency – The Smart Electrical Grid 35
Critical Infrastructure Vulnerability – Teachings from the Aurora Test 37

Broad Critical Infrastructure Vulnerabilities – Notpetya Ukraine 2017 38
Broad Critical Infrastructure Vulnerabilities – Notpetya International 2017 39
Fuel Distribution – Colonial Pipeline 2021 40
Critical system – Critical Infrastructure 41
Global spread mechanisms 42
Global spread mechanism - SCADA systems 44
Discussion 46
Normative Prioritization. 46
The lack of clarity & attribution 48
Cyber as the new military norm 50
Limitations of application of IHL 52
Government and critical infrastructure 54
Conclusion 56
Further Research 60
Bibliography 61

Introduction

In the common imaginary technological risk is often depicted by killer robots and futuristic artificial intelligence, Hollywood movies depicting end of the world scenarios caused by a malevolent supercomputer, and theatrical technologically advanced machines. These often far-fetched notions tend to divert attention away from the often less theatrical reality of human interactions online, and however less exciting or speculative this reality might be, it nonetheless remains a domain that increasingly impacts concrete aspects of society.

Technology has become an increasingly important component of everyday life, having relevance in just about every aspects of society it is hard to envision a path forward without it. This increased relevance is not unilaterally positive, techno-skepticism aside, there are concrete risks associated with the adoption of digital technologies. This project takes a unique approach to assessing the roles, rewards, and risks associated with digitalization of an increasing number of critical tasks in society. By applying the lens of existential risk methodology this project proposes a new perspective to the field of global catastrophic risk by attempting to answer the question: "To what extent can cyberattacks constitute a global catastrophic risk?

This project aspires to contribute meaningfully to the contemporary problem of cyberattacks and offers a normative path forward to the classification and mitigation of a potential cyber-enabled catastrophic scenario. This project aims to fill a gap in existing literature by elevating cyberattacks to the rank of existential risk.

"To what extent can cyberattacks constitute a global catastrophic risk?"

An investigation into the nature, extent, and relevance of cyber-enabled global catastrophic risk.

Methodology

The inspiration for this project came out of a previous interaction with the United Nations Agenda for disarmament "Securing Our Common Future" published in 2018 under the presidency of António Guterres. The agenda covers a wide array of disarmament-related topics, ranging from nuclear disarmament to small arms and light weapons, inspiring nations and policymakers to strive towards a safer world. The third pillar of this agenda, "Disarmament for future generations" includes a section on ensuring peace and stability in cyberspace acknowledging the growing threat of cyber warfare and the exponential impact that cyber attacks can have on society (UN, 2018). In November 2020, Parliamentarians for Non-Nuclear-Proliferation and Disarmament along with the Inter-Parliamentary Union and the Geneva Center of Security Policy published a parliamentary handbook titled "assuring our common future" which supplemented each point made in the UN disarmament agenda with good practices in the field of disarmament (PNND et al, 2020). Working on this publication was my first professional interaction with the topic of cybersecurity and cyberspace, seeking to pursue the issue further academically I wrote about cybersecurity in my 9th-semester project and did a broad exploration of the topic of cybersecurity (Duforest, 2021). This project aims to deepen the methodological and analytical processes to highlight a clear and concise understanding of global catastrophic risks and hopefully provide academic insights into the field of existential risk studies.

This section highlights methodological considerations, the probabilistic limitations, and the choice to pursue a qualitative environmental scanning approach. The methodological consideration will highlight the criteria to which the analysis will relate, and justify the qualitative choices made. The methodology section is concluded by showcasing the means used to undergo the qualitative environmental scan - the CSER's framework of identification of the GCR scenario. The theory section begins with a conceptual framework that will lay down the theoretical foundation on which the paper is built and level the understanding of complex terms such as cyberattack and the asymmetrical nature of cyberspace, the theory section is concluded with a highlight of the Benefit / Dependence / Risk trichotomy which will form the theoretical background of the analysis.

This paper paints a picture of the current reality of interaction in cyberspace, this is achieved by piecing together a non-exhaustive list of attacks demonstrating the extent of the threat faced by society. The cases studied in the analysis section represent a non-exhaustive sample of impactful contemporary cyberattacks, the impact here has been assessed based on physical or cyber damage quantifiable in terms of what was attacked and at what cost, and normative impact in terms of the sociopolitical outcome the attack has had. These are meant to highlight the extent to which cyber warfare can be considered an existential threat, as such, the cases chosen are argued to be consequential attacks, picked to question the fringe and extreme extent of existential risk. Throughout the analysis critical system vulnerabilities will be identified by exploring cyberattack events in-depth, however, shorter cyberattack examples will be used with less depth to supplement points. The cases were chosen accordingly, keeping in mind that due to the nature of cyberspace, one successful and impactful cyberattack in a large sample of unsuccessful ones is not a statistical anomaly, but rather an evidence of a new norm expanding the reality of interactions between physical and cyber. As such, the cases highlight the demonstrated array of possibilities in the field to build up an understanding of what is possible to appropriately help construct meaningful and efficient solutions.

The analysis will apply the qualitative environmental scanning through the CSER's framework. By identifying critical systems in multiple strata of society, their relation to technology, investigating the existence of a B/D/R relation using data, news articles, academic articles, and expert opinions to build an understanding of the level of risk vis à vis cyberattacks. The case study within each sector of society will allow us to derive an understanding of the global spread mechanisms used and available for each scenario. Finally, the analysis will provide an exploration of the risk mitigation failures that are affecting each aspect of society. The discussion section will introduce potential policy-oriented solutions and bring about a deeper understanding of how to address cyber-attacks.

Global Catastrophic Risk.

Global Catastrophic Risk (GCR) is an emerging field of study in international and global politics that has directed attention to a set of human-driven global risks that threaten security, prosperity, and human potential; categorizing events or risks that could jeopardize human security and lead to mass harm and societal collapse (GCRP, 2021). Martine Rees, a co-founder of the Centre for the Study of Existential Risk (CSER) in Cambridge University, associates the growing attention GCR has received from academic circles with the realization that some human technologies are pushing Humanity closer to a "tipping point" beyond which the improbable, but interconnected consequences of an existential risk scenario will cascade globally and cause irreversible human impacts (GCR, 2018). Over the past two decades dedicated working groups and institutions have developed around the topic of GCR, organizations such as the Future of Humanity Institute (FHI), the Global Catastrophic Risk Institute (GCRI), the Future of Life Institute (FLI), and the Centre for the Study of Existential Risk (CSER) have advanced the issue and brought together academics to spread awareness about the topic of GCR. The list of issues mentioned varies from source to source but there is a general understanding across the board on several well-established threats including global warming, ecological collapse, nuclear/chemical/biological warfare, global pandemic, asteroid impact, geoengineering, artificial intelligence, super volcano eruption, including even "non-developed entities" (Bostrom, 2019; Global Priorities Project, 2017; GCF, 2018; Bostrom & Ćirković, 2008). This thesis will emphasize the technological aspect of GCR scenarios, the topics relating to astrophysical processes, geological occurrences, and global warming will not be mentioned beyond the conceptual framework.

Global Catastrophic Risks scenarios are generally understood as having an immense impact with a low probability of occurring, though the probability is never zero. This makes up the foundation of the study of existential risk, the understanding of catastrophic events, and policy-oriented steps towards a total reduction of this likelihood. Plain probability estimates are often used as an instrument to communicate catastrophic risks, Turchin and Denkenberger (2018) argue that probabilistic processes are both inaccurate and inadequate to communicate and measure the notion of existential risk. As Carl Segan points out, existential risk is "not amenable to experimental verification – at least not more than once" (Sagan, 1983). This reasoning aligns with the definition of GCR and the low probabilistic aspect of such an event - making theorizing and

modeling inaccurate and speculative by nature, i.e., a civilization-ending scenario has not yet occurred and its occurrence would leave no one to report on the veracity of the initial probabilistic hypothesis. While the mathematical probability of a natural disaster like an asteroid collision or a geological event can be approximated, most other scenarios remain hard to quantify. This is especially true for technological scenarios which have little hard data and a multitude of often contradictory expert opinions. Not only would a GCR scenario be unprecedented, but such scenario emerges as an interaction between complex environmental, social, political, and economic systems that are hard to independently model and nearly impossible to expose interconnectedly; these factors combined create a high level of uncertainty (Beard et al., 2020). As such, the nature of GCR makes mathematical probabilities an inadequate communication tool to convey the importance and urgency of the topic and have made the quantification of risk speculative and reliant on new creative methods for the analysis of GCR (Turchin & Denkenberger, 2018; Beard et al., 2020).

This epistemic caveat makes the field of existential risk one governed more by political philosophy than by mathematical probabilities, which in of itself is accounted for by the CSER by making the scope of research as broad and encompassing as possible, drawing from the knowledge of experts, and fostering the development of prevention and mitigation strategies in collaboration with academics, industry, and policymakers (CSER, 2021). This interdisciplinary approach is vital for effective coverage of all possible sources of the emergence of a GCR scenario.

Methodological considerations

Academic literature on the methodological consideration in the field of existential risk offers various approaches to the quantification of GCR scenarios. Beard et al. (2020), and Tonn and Stiefield (2013) will be the ground literature for the methodological considerations. Both authors express similar concerns about the limitations of a mathematically rooted methodology in relation to existential risk assessment.

Beard et al. (2020) have surveyed the literature on the quantification of Existential Risk and provide four criteria for the evaluation of an existential risk methodology: rigor, uncertainty, accessibility, and utility. Rigor is the ability to access a broad range of information and expertise from multiple perspectives, the suitability of their means for turning this into a final judgment, and

the ease of incorporating new information into this judgment or combining different judgments using the same method. Uncertainty being the ability to deal with uncertain data, whether the methodology provides confidence in their estimates and helps identify epistemic bias. Accessibility relates to the ease of applicability of the methodology concerning the growing field of ER/GCR study and the general number of barriers to application. Lastly, utility, which relates to the ability to yield credible, insightful, and useful information that can be used in policy selection and prioritization and easily communicated to varied stakeholders (Beard et al., 2020). These criteria will be applied to the shaping of the methodology section as a whole and be the standard this paper aims to attain.

Environmental Scanning

The environmental scanning methodology has for main purpose the identification of information that can provide insight about how the future will unfold, these insights are then used in strategic planning to ensure that one's organization can adapt and prosper in the future (Tonn, 2007). In the environmental scanning approach, the assessor builds a multiple-components causal model of human extinction, scans human knowledge bases for "leads" that influence the components, estimates the influences of leads over components, and aggregates influences through the model (Tonn, 2007). It is important to acknowledge the sheer amount of available data that can constitute a potential lead, due to this diverse and immense array of available data, the environmental scanning method has not incorporated any tools to guide the breadth and depth of the scan. The method preconizes gathering from as diverse a set of sources that pertain to the question at hand, in this case, finding a comprehensive answer of the likelihood of human extinction due to an event relating to cyberattacks. This methodology allows the user to estimate quantitatively the impact of each lead upon the organization, assess uncertainties associated with the impacts, and aggregate the impacts of each lead into a total impact report upon the organization (here society). The methodology as introduced by Tonn and Steifel (2013) is also efficient when used qualitatively, this is supported by the work of Rees (2008) and Bostrom (2002) who have approached the topic of existential risk in their field through a qualitative environmental scanning method.

Quantifying impacts of leads on components - Numerical association

The initial environmental scanning methodology requires the researcher to identify lead components that can affect the system being investigated. Once identified the lead is assigned an arbitrary number ranging from +10 (positive impact) to -10 (negative impact) to assess and quantify the degree and nature of the impact that the lead change has on the investigated system. Considering the arguments made earlier regarding mathematical probabilistic ratings, this step will not be included, and the quantitative numerical rating will be supplemented by a qualitative expert opinion and cases studies, the leads will be assessed according to their impact (negative or positive) on the eventuality of a GCR scenario. This trade-off decreases the subjective nature of the methodology but limits its replicability, in this instance the trade-off strengthens the project overall since it aims to brings forth an educated and exploratory investigation of cyberattacks as a GCR scenario. The outcome of this study will therefore not be probabilistic but rather a heuristic aggregate of the technological influences and an estimate of the risk they pose to society.

Classification of Global Catastrophic Risk

This paper will apply the environmental scanning methodology through the framework presented in "classifying global catastrophic risks" by Shahar Avin, Bonnie C. Wintle, Julius Weitzdörfer, Seán S. Ó Héigeartaigh, William J. Sutherland, and Martin J. Rees. This joint publication from the CSER introduces a framework of identification of Global Catastrophic Risk scenarios by analyzing and identifying three core aspects: critical system affected, global spread mechanism, and prevention and mitigation failure (Avin et al., 2018). The classification system highlights convergent risk factors that merit prioritization and uncovers potential knowledge gaps; it also brings policy implications for research agendas and prevention and mitigation prioritization, which will be used more extensively throughout the discussion section.

Critical system

A critical system is defined as any system or process that, if disturbed beyond a certain limit or scale, could trigger a significant reduction in humanity’s ability to survive in its current form (Avin et al., 2018). The classification of critical systems is done according to a hierarchical framework

that differentiates between “higher-level” systems, the overarching systems that are comprised of the “lower-level” systems. As such a critical system ensuring socio-technological processes such as the global market infrastructure might depend on sub-systems at a lower level such as functioning utilities, resource extraction, or distribution of basic goods and services (Avin et al., 2018).

The identification of a critical system is to be achieved through expertise in a field relevant to the subject at hand, for the purpose of this project and in the context of cyberspace, emphasis will be primarily placed on the socio-technological critical systems. The analysis will explore societal cyber fragility and assess the GCR by highlighting contemporary cases and scenarios in the military, governmental, societal, infrastructural, and private sectors. Applying knowledge from the theory section, expert and academic inputs, and various news reports to bring together an estimate of which critical systems of society are under threat and/or vulnerable to cyber disruption. The categorization of identified critical systems could be done in multiple ways, these categories were picked to cover the broadest scale of society, note that the critical systems identified have relevance in multiple overlapping areas of society, the decision to place critical systems under these categories relates to improved clarity, but they must not be thought of as entirely isolated from one another.

Global spread mechanisms

The failure or impact of an event on a local critical system is rarely enough to pose a GCR scenario in itself – a regional crop failure remains a local issue until coupled with a global spread mechanism. This purposeful separation between critical systems and global spread mechanisms allows us to identify details in the GCR scenario mechanisms and means to manage and control them (Avin et al., 2018). Global spread mechanisms are the way through which an event or system failure spreads worldwide. Global spread mechanisms can be natural, but the authors highlight the importance and potential impacts of emerging technologies and man-made spread mechanisms like the internet or airports (Avin et al., 2018). The internet and digital technologies will be the main highlighted global spread mechanisms considered for this project.

Global spread mechanisms can also be thought of as enablers for GCR scenarios, a case mentioned by the authors is the enabled access to impactful technologies whereas anyone could

theoretically run a "do it yourself" bioengineering project or a hacking software (Avin et al., 2018). The authors offer a non-exhaustive list of types of critical systems and forms of global spread mechanisms and establish a cross-referencing grid where the type of critical systems meet types of global spread mechanisms to account for a range of scenarios including, but not limited to an asteroid impact, ecological collapse, nuclear war, hostile artificial intelligence, natural and man-made pandemics, or volcanic eruption (Avin et al., 2018).

This theoretical framework will be used primarily to identify the types of critical systems affected and how cyber-attacks can have impacts globally, the identification elements for these two factors will be built from various sources relevant to the field of cybersecurity, digital governance, warfare, and emerging technologies.

Prevention, and mitigation failures

This aspect of the framework accounts for the human aspect regarding the attention given to matters of GCR by assessing the road stops and existing biases that make mitigation and prevention endeavors fail, or less efficient. Including the cognitive bias of risk, perception extends the scope of answers available when addressing the policy issue which helps steer the scope of risk-mitigation options, and while some GCR scenarios like pandemics, natural disasters, floods, hurricanes, or droughts, are already well known and accounted for in institutional system there is growing attention placed towards emerging technologies since the field lacks research and has no concretely established agenda (Avin et al., 2018).

For GCRs from emerging technologies, however, the institutional mix and a research agenda are only just becoming established, meaning that exploring the mitigation and prevention failures can highlight the existing shortcomings of institutions or individuals (Avin et al., 2018). Identifying the prevention and mitigation failures will is the final part of the framework and is the third component of the assessment of global catastrophic risk.

Theoretical Background

This section relates to the first step of the CSER Global Catastrophic Risk Policy paper: understand. "Governments must sufficiently understand the risks to design mitigation, preparation and response measures." (GCR, 2018). As such, this section attempts to build a ground theoretical understanding of the digitalization processes and provide the necessary understanding of the nature of cyberspace and cybersecurity to move forward in approaching the cases in the analysis section.

Benefit/Dependence/Risk theory

This section links the technological progress (mainly digitalization) with three interconnected consequences: benefit (improved in quality, time, and efficiency of a given task), dependence (an evolution of the sector towards more digitalized technology), and risk (the nefarious consequences this change can bring about i.e., vulnerabilities). This idea is the theoretical starting point of this paper, and the pattern of benefit, dependence, risk will be tested and explored at length throughout the analysis.

The adoption of the Internet of Things (IoT) throughout the 21st century has allowed for many everyday appliances and working environments to become connected and intertwined. There is no doubt that such connectivity came to be adopted for its many benefits, improved efficiency, faster interactions, and new possibilities (Rivera, 2020). In the contemporary cyber context, connectivity means exposure and can often bring about levels of cybersecurity threats to the device and its user (Rivera, 2020). This connectivity caveat has been applied to the adoption of IoT devices used in commercial and consumer environments but relates equally to the broader scope of digitalization. "With the technological progress and the rewards that come with the information age comes new risks and consequences that need to be better understood and managed" (Horton, 2003). As this project will explore this trend applies equally to militaries, governments, infrastructures, and private sectors and for "as long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk" (Libicki, 2009). This is not to be understood with techno-skepticism or a modern form of Luddism, technological progress is a forward-moving force regardless of oppositions. This idea is used throughout this paper as a cautionary note, brought forth to raise awareness of existing vulnerabilities in digital systems, rather than seeking to dispense with them altogether.

Cyber has its own rules.

Cyberspace is a rather ill-defined concept, building a theoretically grounded understanding of the nature of cyberspace will allow us to better understand the interactions that take place in this realm and more accurately identify risks that can arise within it. Cyberspace is not a physical space, and while elements of cyberspace are bound to physical locations in objects such as servers, computers, drives, or other appliances; it is the digital content of these physical objects that constitutes what we call Cyberspace (Clark et al., 2014). A conceptual reasoning borrowed from Thompson (2012) helps understand the nature of cyberspace as this all-encompassing technological realm that has overarching reaches and is best described as being "performative" in the sense that it is defined not by what it is but by what is done with it. Cyberspace is comprised of a multitude of Information and Communication Technologies (ICTs), such as computers, phones, servers, and any other digital devices connected to the internet forming a web on which users interact. Companies (large and small), organizations, and individual citizens are all moving towards a growing dependence on ICTs to efficiently complete critical tasks (Clark et al., 2014). The reality of interactions in cyberspace has been theorized by Martin Libicki (2015) who argues that the human component of technological advances in cyberspace creates a divide between the intended usage of digital technologies in theory and the actual uses of it in practice. This idea becomes even more relevant with the increase in complexity of algorithms and software whose intricacies leaves room for unintended uses of programs, leading technology to do exactly what code dictates rather than what the designer or operator intended (Libicki, 2015). Entry pathways in a secured system are often due to an oversight or a flaw in the system which are endemic to man-made digital systems - one saving grace is that these design flaws can be corrected, however, a caveat remains that most of the time it is done so after having been abused or breached (Libicki, 2015). These are called Zero-Day Vulnerabilities, a flaw in a system that makes itself known only once breached, if these are not discovered and patched in time, they can lead to Zero-Day Attacks. Zero-Day Vulnerabilities are almost a natural constituent aspect of modern digital systems, since digital technologies have increased in complexity beyond a threshold of natural human comprehension, making the human element a considerable fallible element in modern digital systems.

Cyber security

Understanding the concept of cybersecurity helps to pin down and curtail the notion of cyberspace. The International Telecommunication Union defines cyber security as the collection of tools, policies, security concepts, security safeguards, risk management, guidelines approaches, training, actions, best practices, assurance and technologies used to protect the cyber environment and organization and user's assets – including connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment (ITU, 2008). However, the extent of cyber security is not only limited to digital information but includes the impacts on physical entities as well as individuals, Solms and Niekerk (2012) argue that humans in their personal capacity and society at large can be directly harmed or affected by cyber security attacks. There is a line to be drawn between information security and cyber security. Information security refers solely to the protection of data and information on cyberspace, which are assets in of themselves, from possible harm. Whereas cybersecurity extends this protection further to human and physical objects that function and interact on the cyberspace (Solms & Niekerk, 2012). Private sector companies, as well as governments often struggle to keep up with the pace of development of cyberspace and the evolution of cyber security threats. Thus far, most strategies and action plans to provide lasting security in cyberspace have fallen short, highlighting the technological offensive-driven reality of interaction in cyberspace (Shore, 2015).

Asymmetrical interactions refer to a form of unbalanced, some might say unfair interaction between two actors, in the context of cyberspace the asymmetry between a perceived attacker and defender shines in multiple ways. In cyberspace asymmetry is characterized by one key aspect: attribution. Using digital tools such as a proxy, bot, or virtual personal network a cyber attacker can effectively and cheaply conceal its internet protocol address (IP), allowing critical information such as location or identity to remain hidden. Cyberattacks can be launched from literally anywhere, including cybercafés, open Wi-Fi nodes, and suborned third-party computers, leaving no tangible traces behind (Libicki, 2009). This ability to launch an attack or test defenses repeatedly while remaining beyond the grasp of detection constitutes the attribution problem of relations in cyberspace. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) mentions a practical case where a citizen from country A, uses a proxy in country B to target

information of a citizen or organization in country C that is stored in country D while operating from country E. This theoretically endless network of connection renders attribution nearly impossible, adding to the fact that while detection and attribution technologies are evolving, the technical environment in which they are deployed is so dynamic that attackers often remain out of reach (Banks, 2017). Carlin (2016) takes this reasoning further by exposing a case where a hacker can use a proxy in the middle east to launch an attack on a U.S. organization creating a scenario where the attack could be miss attributed to a middle eastern country – heightening the complexity of attribution of cyberattacks (Craigen et al., 2014). The ability to remain hidden leaves entities, whether a governmental organization or a rogue individual, to operate in cyberspace with impunity. The lack of global expertise and established framework for the categorization of cyberattacks benefits cyber-abled states allowing them to operate freely in a realm that is unregulated and unsupervised (Carlin, 2016).

Analysis

Following the structure laid down in the methodology, the analysis will apply the environmental scanning and the classification of global catastrophic risk to identify and highlight the cyber vulnerabilities of multiple aspects of society. The first chapter of every section is focused on identifying the evolution of technology in the relevant field by laying down concepts and academic perspectives. The identification of critical systems in the field is then established with in-depth case studies highlighting cyberattacks and exposing vulnerabilities.

Public Sector Administrative Governance

As the centerpiece of decision making governments have been adopting measures of digitalization of their functions in an effort to improve the speed, quality, and range of their services. Digitalization of essential public functions has been witnessed historically within developed governments and more recently within developing countries (Björklund, 2016). This trend is commonly referred to as e-governance – the use of information and communication technologies within the public sector. This entails digitalization of government records, national data, as well as communication between government, public administration, and citizens (Björklund, 2016).

Research done on the effects of implementing e-governance all point towards progress at various levels of the public sector.

E-governance allows for the public services to be cheaper, faster, and more widely available to the citizens, this gain in efficiency is also paired with a gain in effectiveness rendering public governmental services more innovative and more efficient (Heeks, 2001). The administrative processes are improved by digitalization, the case of Egypt in the early 2000s is often referred to when assessing the benefits of e-governance. The digitalization of national data allowed over 130 million entry points on births, deaths, marriages, and divorces that allowed for the creation of a country-wide ID card system that paved the way to further expand the range of public services at a significantly reduced cost (IDSC, 2000). E-governance also improves the connectivity between citizens and governments, allowing the citizens to stay informed of public sectors activity and to a certain extend reinforce accountability of the politicians (Heeks, 2001). The improved communication allows citizens to voice their concerns much more directly improving the services delivered to members of the public along dimensions such as quality, convenience, and cost (Heeks, 2001). Finally, e-governance allows governments to build external interactions much more easily, developing communities and building partnerships. A clear positive correlation between digitalization and productivity has been established at the governmental level. Alexandrov et al (2019) have found that the trend of digitization is in direct correlation with increased productivity in early adopting countries, whereas recently digitized governments will not see the positive impact until the later stages of the digitization process. The UN e-governance survey published on a yearly basis equates e-governance with “opportunities to support the achievement of the 2030 Agenda and the Sustainable Development Goals, including by enhancing the efficiency and effectiveness of public service delivery and by reaching those left behind” (UN, 2020).

The UN e-government survey uses the e-government development index (EGDI) as a measuring tool to quantify the levels of digitization of governments around the world. The EGDI is a weighted average of various dimensions of e-government namely, the Online Service Index (OSI) which is scope and quality of online services, the Telecommunication Infrastructure Index (TII) which is the status of the development of Telecommunication Infrastructure, and the Human Capital Index (HCI) which is the inherent Human Capital of the country. The formula is as follows:

EGDI = 1/3 (OSI + TII + HCI). The global average EGDI value increasing from 0.55 in 2018 to 0.60 in 2020 (UN, 2020). This average global progress is also witnessed in least developed countries (LDCs), landlocked developing countries (LLDCs) and small island developing States (SIDS) amongst these categories very high EGDI values (above 0.50) has increased by 29 per cent since the last 2018 edition of the survey. This trend in digitalization of governance is a global phenomenon which is arguably on a set course for current and future modes of governance, progressively digitalizing key aspects of governance.

Broad Governmental Vulnerability – The Case of Estonia 2007

Estonia is to this day one of the countries with the highest EGDI (0,9473) (DESA, 2020). This national trend in digitalization begun as an effort to modernize the governmental infrastructure following the Estonian separation from the soviet bloc in 1991. E-government was developed through close cooperation between private and public sectors, the investments in informational infrastructure was made possible by some favorable economic developments, but the trend of e-governance was also in line with the process of strengthening democracy after a long period of extraneous authoritarian rule (Björklund, 2016). Estonia quickly adopted online banking, online registration, online ID, internet-dependent infrastructures, online tax returns, computerized official government meetings, and progressively moved vital aspects of public life online (Haataja, 2017). Estonia's stance on digital governance is outlined in their digital agenda where they state being a "global champion of digital living" dating that trend all the way back to 1994 with the first governmental policies in digitalization of "information policy" (EAS, 2021).

This extensive digitalization made Estonian public services prime targets for cyberattacks and in 2007 showed to be a serious vulnerability (Haataja, 2017). The attack begun on the 27th of April 2007, following a protest by the ethnic-Russian minority in the capital city of Tallinn over the displacement of a commemorative soviet statue from the second world war. The waves of attacks begun late April and lasted until mid-May 2007. A variety of governmental and political websites including the presidential website, Prime Minister's website, Homepage of the Parliament, most government departments, political parties, and media organizations were targeted by a distributed denial of service attack, rendering them unusable (Haataja, 2017; Tikk et al., 2010).

The communication infrastructure was also impacted, the national Domain Name Service (a key national component of internet browsing) and the overall internet infrastructure and information technologies were targeted (Haataja, 2017). Local media web outlets and the Estonian government's online briefing room were among the first sites to come under cyberattack, at the time major international media companies related Estonian news exclusively through the government newsroom, reducing the international and national coverage of the case as the attack took place (Tikk et al., 2010). Commercial Services like the E-banking services of Hansapank and SEB Eesti Ühispank, the two largest Estonian banks were attacked intermittently throughout the period of April-May 2007. Given that in 2007, the share of electronic transactions amounted to about 95-97% the attack rendered online banking systems unusable (Tikk et al., 2010). Emergency lines and telecommunication services were also impacted throughout the attacks (Haataja, 2017; Tikk et al., 2010). The purpose of the attack was mainly disruptive, no lives were lost as a direct consequence of the attack and the damage remained mainly monetary, some estimates quantify the economic impact of the attacks at between 27 to 40 million USD (Haataja, 2017). According to the Estonian Information System Authority (CERT-EE) the attack was clearly meant to disrupt while remaining hidden, the malicious online traffic originated from a multitude of IP addresses located in 178 different countries (Tikk et al., 2010). While the political tensions that preceded the attack have allowed investigators to speculate on Russian involvement no tangible link has been established with the Russian government. However, log analyses affirm that the cyberattack required resources and coordination that are not by default available to a "regular citizen"; leading experts to believe that a sophisticated command and control system was put in place (Tikk et al., 2010). Some Russian-ethnic citizens were arrested and charged for minor parts of the attack, but the attribution of the 2007 cyberattacks remains uncomplete.

The 2007 Estonian cyberattack became a wake-up call for many in the international community, NATO helped fund the CCDCOE in Tallinn a year after the attacks. The center would go on to gather lawyers, experts, professionals, and academics in the field of cybersecurity to write the Tallinn Manual, which will be further discussed in the discussion. Toomas Hedrick Ilves, the president of Estonia in 2007 would go on to call this attack "web war I" and spoke out publicly about the importance of cyber security. The Estonian attack was the first of its kind, and Estonia was in a particular position making it a vulnerable target but their efforts in digitalization allowed them to recover with no long-term effects on governmental services. Estonia's Digital agenda

continued to evolve, focusing on cybersecurity in 2008, expanding core services like healthcare and medication prescriptions to an online platform between 2008 and 2010, rolled out a "data-embassy" program that backs up state data in case of failure or attack in 2015, and even started implementing AI solutions to governance in 2019 (EAS, 2021). The case of Estonia really serves the argument of CGR and cybersecurity by introducing the early extent of possible points of vulnerability in a digitalized government. The ability for a government to communicate with its citizens, and for the citizens to remain informed of a given situation, whether through the government portals or the media is a key aspect of modern society. This case also highlights the lack of alternative options governments can turn to in the event of a cyberattack rendering communication unstable, or unusable. The digitalized online public services were also impacted, the ability of the government to provide public services was altered throughout the duration of the attack impairing a key aspect of governance.

Governmental Agency Vulnerabilities - The Solar Wind Hack 2020

In December 2020 Russian hackers were found to have successfully infiltrated the Solar Wind software, this impacted over 200 organizations around the world which were using the application to run key tasks. (CSIS, 2021). A BBC article interviewed cybersecurity experts on the hack, and it is believed that upwards of 18,000 organizations, including fortune 500 companies and governmental organizations, have been impacted by the cyber-attack (BBC, 2020). The Solar Wind app is used for configuration management and acts at the center of the digital framework of the organization by helping the user with handling firewalls, security details, logins, passwords, and credentials. The malware used for the cyberattack is thought to have been introduced into the solar wind system as early as September 2019 and remained undetected for more than a year during which malicious code was integrated to the software of thousands of organizations (Avena, 2021). This cyberattack has been qualified as one of the most sophisticated coordinated attack, the scale and scope of the attack has led the cyber experts of Microsoft to speculate that upwards of thousands of hackers worked on the attack over the span of a year (Avena, 2021).

"Primary indications suggest that the scope and scale of this incident are beyond any that we've confronted as a nation and its implications are significant" said senator Mark Warner of the Select Committee on Intelligence chair of the panel's first hearing on the Solar Wind cyberattack

(PBS NewsHour, 2021). While the attack left no physical damage on any of the infrastructures impacted it allowed the hackers to have unrestricted access to the content and data of the organizations, among which was the US National Nuclear Security Agency, the agency in charge of securing and overseeing the US's nuclear weapon stockpile and the Department of Energy the agency in charge of energy and safety in handling nuclear material (Bertrand & Wolff, 2020). Experts in cybersecurity acknowledge that the cyberattack could have deeply impacted the target organizations since the software was essentially the control point of the security framework, a "worst case scenario" could have realistically left the organizations defenseless or impaired. The Department of Energy insisted that the malware "has not impacted the mission essential national security functions of the department, including the National Nuclear Security Administration" (Bertrand & Wolff, 2020). Former homeland security officer, Tom Bossert, expressed concerns over the extent of the hack stating that it could take years before establishing and ensuring the networks security levels and that the hackers could "destroy or alter data, and impersonate legitimate people" (Bossert, 2020). Bossert also recommends a "do over" of governmental security infrastructure as the only secured solution to the breach, fully acknowledging that this remediation effort comes with a staggering cost and impact (Bossert, 2020).

This cyberattack really showcases the extent of modern security frameworks and highlights the inherent vulnerability of man-made cyber systems mentioned by Libicki (2015). Many hailed the Solar Wind software as one of the most secure on the market, and its breaching raised a lot of questions on the nature of governmental security and the ability of agencies to safely preserve national data from being exfiltrated by malicious actors.

Critical systems

The critical systems highlighted in this section relate to the ability of governments to carry out key functions pertaining to the smooth running of society. Firstly, the communication aspect which relates to the government's ability to communicate with its citizens whether through direct communication or through upholding the structural integrity of communication systems for media companies to do so. The case study of the Estonian attack of 2007 highlights the attack of government websites and media companies, but this is not an isolated case. February 2020: Iran announced that it has defended against a DDoS against its communications infrastructure that

caused internet outages across the country; June 2019: a suspected Iranian group was found to have hacked into telecommunications services in Iraq, Pakistan, and Tajikistan; December 2018: Chinese hackers were found to have compromised the EU's communications systems, maintaining access to sensitive diplomatic cables for several years; October 2018: the Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government Groups (CSIS, 2021). These examples and the case study show that as a critical system, communications are vulnerable to cyberattacks.

As to the overall security of government agencies, the impact on communication as well as the upholding of information relating to national security have also been proven to be vulnerable to cyberattacks. The Solar Wind hack is the most recent instance of a breach on governmental agency, but there are many other cyberattacks of the same nature that could have been used as a case study. April 2018: Security researchers report that an Indian hacking group had been targeting government agencies and research institutions in China and Pakistan since 2013; October 2017: a major wave of ransomware infections (associated to the NotPetYa) hits media organizations, train stations, Centre for airports, and government agencies in Russia and Eastern Europe; August 2016 weeks before legislative elections in Hong Kong): two Hong Kong government agencies were penetrated in an attack allegedly by China (CSIS, 2021). The reason why the Solar Wind hack stands out is that most cases of cyberattack on government agencies are confined to espionage or disruption, the nature of this attack could potentially have damaged the security infrastructure of US agencies and of the impacted organizations to a point beyond repair.

An element of vulnerability that has not been assessed in this chapter but remains nonetheless relevant is the mediatic impact of cyberattacks on democratic processes. The 2016 DNC emails hack, as well as the 2017 French election interference are just two examples of event where documents were obtained via cyberattacks and leaked to the press to destabilize democratic processes.

Military systems

Since the 1970s Information and Communication Technologies (ICTs) and digital technologies have become an increasingly crucial part of military command and control. The integration of digital technologies has allowed military operations to transform the defense industry, advances like smart weapons, real time battlefield management, network-centric solutions, superiority in air and outer space, and software-based solutions to ground troops all have key roles today. ICTs remains a key enabler to gain more effect from units composed of men, procedures, machines, software, and information (Mattila & Parkinson, 2017). In 2020, the French Senate hosted French military officer Thierry Burkhard who gave an exposition of the French army's plan for the years to come, in this plan he introduced the Orion exercise aiming to prepare the army for an eventual major military confrontation. Exercise Orion is set to take place in 2023 and will involve the full range of the French military capacity on a scale that has not been witnessed in decades. Burkhard also stated that "the use of information warfare is now systematic in all confrontations" stressing the importance and reliance of ICTs in modern military (Labialle, 2020). This trend of digitalization has been and to a large extent is still being applied to the classical military domains (air, sea, land), but recent trends have showcased a diversion of technological attention away from the physical military systems and towards cyberspace.

Digitalization of the Military – Offensive Cyber Capabilities

Digitalization and the rise of cyber-enabling tools for military systems has received an increased amount of attention from militaries around the world. The proliferation of cyber operations as a military tool is currently impacting the way military strategists and leaders perceive warfare and interact on the international scene. Lin and Smeets (2018) are two academics working with the Center for International Security and Cooperation and Stanford University, their research on Offensive Cyber Capabilities explores the impact that cyber-enabled technologies have on the traditional distribution of power and influence classically attributed to physical tools of warfare. They define OCC as "a capability designed to access a computer system or network to damage or harm living or material entities" (Lin and Smeets, 2018). This definition implies the exclusion of espionage but as we will see later the boundary between offense and espionage is often blurred.

Instead, Lin and Smeets focus on the type of damage caused by the attack, whether denial of service, damage file, or physical damage.

When assessing the impact that the adoption of cyber-capabilities has on traditional military systems one must first understand the classic uses of traditional offensive capabilities namely Defence, Deterrence, and "Compellence" (Lin & Smeets include "swaggering" as a fourth aspect but this paper will not take it into account as it relates to prestige and cannot really be applied to cyber). Robert J. Art (1980) wrote "to what end? Military powers" in which he explores the traditional uses of military powers, this is the base form which Lin and Smeets evaluate the impact of cyber-enabled technologies. Centre of Excellence (CCDCOE) released their 2018 report in which they assessed the impact of Offensive Cyber Capabilities (OCC) on the roles of military power. OCC are defined as "a capability designed to access a computer system or network to damage or harm living or material entities" note that this definition excludes espionage, information warfare and information operations from the scope of analysis.

Defensive applications of OCC can be used to avert an attack or minimize damage of an attack. For defensive purposes, a state can deploy its forces in place prior to an attack, use them after an attack has occurred to repel it, or strike first if it believes that an attack upon it is imminent or inevitable (Art, 1980). A distinction needs to be made between pre-emptive and preventive strike, where the former refers to a believed attack from an enemy is imminent, the later refers to an attack that is perceived as inevitable or has been proven to be planned.

Deterrent uses of military force aim to dissuade an adversary from doing something by threatening him with unacceptable punishment if he does it, deterrence relies on a credible threat of retaliation and as Broady (1958) argued "must be always at the ready, yet never used." Conventional deterrence relies, amongst other things, on credible military intervention, the threat of use of nuclear weapons, or economic sanctions. The transitory nature of OCC differentiates it from conventional means of deterrence, technical (type of vulnerability, access and payload used) and non-technical (the number and type of actors the capability is used against) factors determine the temporal nature of OCC. Another factor to consider is the clandestine nature of OCC, an announced attack is often rendered useless and the capability itself is only proven post-deployment (Lin & Smeets, 2018). These two factors make nation states and militaries reliant on speculative talk and "cheap talk" to convey the notion of deterrence. This links back to Thompson's idea of

cyberspace being a performative space, a nation can showcase a new weapon in a military exercise but is left to relate to the performance of a cyber attack to convey the idea of deterrence. Accordingly, deterrence in cyberspace is left almost exclusively to reputation and credibility which is itself built through the post-deployment results. In this aspect the international scene gains a theatrical aspect where nations try to prompt each other's cyber defenses in an attempt to build up a credible cyber offensive performance to establish a reputation as a cyber-abled state. In relation to traditional deterrence, cyber deterrence is a less effective tool of power relations since it relies on perceived reputation rather than concrete offensive capabilities.

Finally, Compellence, which is a term that was coined by American economist Thomas C. Schelling in 1966, Schelling described compellence as a direct action that persuades an opponent to give up something that is desired. The compellent use of military force serves one of two purposes: i) to stop an activity undertaken by an adversary, or ii) to get an adversary to do something he has not yet undertaken (Lin & Smeets, 2018). Deterrence relies on use of force based on a perceived threat and the promised automatic reaction to an attack, whereas compellence places more strategic power on the threatening party to achieve a given goal (Lin & Smeet, 2018; Schelling, 1967). Cyber capabilities have by nature particular advantages allowing belligerent states to relate to the compellent use of cyber capabilities differently than they would to a traditional use of military capability. Namely: *reputational damage* – the compelled state can undergo the attack without publicly admitting it (e.g. dismiss the event, or present it as a technical failure); *expansion of impact* – the attack needs to be consequential enough to appear as a credible threat; *reversibility* – the attacker can offer to retrack the cyber-attack (or threat) if demands are met (Lin & Smeets, 2018).

The adoption of OCCs has impacted some aspects of Art's traditional military offensive capabilities (defense, deterrence, and compellence). First, the tactical potential of OCC as pre-emptive and preventive strike is increased by the nature of cyberwarfare, this re-emphasizes the potential use of force for defensive purposes. Second, the role of deterrence has been downgraded by the adoption of OCCs, linking this argument with the performative nature of the cyberspace, states and governments are depending on displays of force to build credibility on the international scene. Lastly, OCCs have brought forth the idea of compellence as a credible power relation tool, allowing states to operate and influence sovereignty with these newly adopted cyber pressure tools

with an option to keep it away from public scrutiny. The adoption of OCC by the military has brought cyber warfare to the attention of military leaders as a tactical tool for with heightened flexibility and greater use of application. The Cooperative Cyber Defence The CCD COE argues that the increased interest in OCC has the potential to profoundly impact the way military responses are carried out and has downgraded the role of deterrence. Unlike conventional capabilities, the effects of offensive cyber capabilities do not necessarily have to be exposed publicly which limits the eventuality of having to be highlighted on the international scene. The CCD COE categorizes cyber-attack cases according to which type of damage they incur denial of service, file damage and physical damage (Minárik et al., 2018). These will be expanded further in the next chapter.

Military Applications of Cyber – NATO

In the 2016 Warsaw summit NATO officials acknowledged cyber-attacks as a clear challenge to the security of the Alliance and placed cyber-attacks on par with conventional attacks when maintaining collective defense. The Warsaw convention also was used to reaffirm cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea (NATO, 2016). NATO has announced the expanding of the capabilities and scope of the NATO Cyber Range, where Allies can build skills, enhance expertise, and exchange best practices (NATO, 2016). Other individual states across the world including Belgium, Columbia, Germany, Finland, India, the United Arab Emirates and Vietnam have all said they are exploring options for cyber warfare, while the United States, China, Russia, Israel, the United Kingdom, Iran and North Korea continue to further develop their offensive cyber capabilities (Lin & Smeets, 2018).

In 2018 the US office of Cyber Command released a military strategy document emphasizing the tactical importance of cyberspace in military operations stating that “achieving superiority in the physical domains in no small part depends on superiority in cyberspace” (USCYBERCOM, 2018). “As the 2018 National Defense Strategy explains, adversaries are increasingly capable of contesting and disrupting America’s society, economy, and military - this is in part because of our growing reliance on cyberspace” (USCYBERCOM, 2018). In 2018 the Trump administration signed into effect the National Defense Authorization Act (NDAA) which

blurred the traditional distinction between Title 10 (Armed Forces) and Title 50 (War and National Defense) authorities, allowing the DoD to conduct coercive and covert actions with less restraints and often without congressional or executive approval (Bailey, 2020; Pomerlau, 2019). The boundaries between what is considered cyber-enabled espionage and intervention are blurred and leave the DoD to operate in a grey zone that could be considered interference in the domestic affairs of foreign sovereign powers.

Over the past couple of years China has also been investing in cyber defense and offence tools but has primarily used its cyber capabilities for espionage (Jinghua, 2019). The stance that China has adopted in cyberspace carries some adversarial implication towards the US. On the one hand cyberspace continues to be a major catalyst for economic growth, technological innovation, and social development around the world; and China is determined to use it as efficiently as possible to reap these benefits (Lindsay, 2015). On the other, Communist censorship is undermining the democratic promise of information technology, and the CCP is pointing out the dominance that American firms have online and has tried to exempt the west from its cyber bubble (Lindsay, 2015; Jinghua, 2019).

Military Applications of Cyber – Russia

Russia is omnipresent in cyberspace, whether as an alleged or verified attacker, the CSIS offers a database of major cyberattacks since 2005 and mentions Russia over a hundred times (CSIS, 2021). Later chapter will explore concrete cases of cyber attacks some of which involving Russian government-sponsored hacking, but this chapter is meant to specifically explore Russia's relation to cyberspace and their military stance towards OCC.

Throughout the past decade Russia has been taking full advantage of the tactical benefits provided by the nature of cyberspace as a medium of operation, invoking plausible deniability through the difficulties of attribution, launching attacks at a diminished cost, and exploiting the asymmetrical nature of cyberattacks. Lilly & Cheravitch (2020) have compiled a comprehensive analysis of Russia's policy and doctrine relating to cyberwarfare based on official documents, media portrayal, and investigative works of the actors responsible for executing cyberattacks and digital influence campaigns. Within the current international context, particularly in relation to

NATO and the defensive alliance that it forms, Russia has been taking full advantage of OCCs as a tactical tool to operate in an undefined grey zone of what constitutes aggression by consistently playing on the line between asymmetric interstate competition and full-out conflict. Russia's cyber posture is reflected in the offensive cyber operations launched by Russian government departments (mainly the Main Intelligence Directorate "G.R.U."), whose institutional culture, expertise, and modus operandi have affected and will continue to affect Russia's cyber signature on the international scene (Lilly & Cheravitch, 2020). This is further illustrated by the Russian military scientist who evoke a growing attention given to the development of cyberweapons due to their effectiveness, appropriateness within the framework on contemporary conflict, and affordability. Russia is similar to other nations in the sense that it has adopted information and cyber warfare as an integral element of modern military doctrine but differ from other governments in how it depicts itself as adhering to defensive postures in an environment characterized by aggressive adversaries (Lilly & Cheravitch, 2020). Acknowledging the uses of OCCs and more specifically the downgraded role of deterrence and the reliance on state credibility to use OCCs the case of Russia shines as a perfect example. The recent military intervention of Russia in Ukraine has allowed it to test out and demonstrate its OCCs relatively unchallenged and establish credibility as a cyber-capable nation.

Military Vulnerabilities on the Field – The Ukrainian D-30 Howitzers

Crowdstrike is an American firm specialized in cybersecurity breaches, it identifies and analyses various hacking tools and devices along with offering protection services to companies and organizations. Their efforts in identifying entities in cyberspace is recognized by many experts and has played a key role in many investigations, their work will be used to introduce FANCY BEAR. Fancy Bear is a Russian nation-state adversary group that has been operating since at least 2008, the group poses a significant and consistent threat to organizations around the globe – specifically by targeting extensive operations against defence ministries and other military victims, which seems to indicate a link with the Russian Main Intelligence Department (GRU) (Crowdstrike, 2019). The primary tool developed by the Fancy Bear group is a hacking implant called "X-agent" which allows them to export malicious code into the affected devices, X-Agent is also a cross-platform remote access toolkit, variants of the tool have been identified for various Windows operating systems, Apple's iOS, and likely the MacOS (Meyers, 2019).

One application of the X-agent implant by the Fancy Bear group was witnessed between 2014 and 2016 in Eastern Ukraine during the Russo-Ukrainian conflict over Crimea and in the Donbass area. The Ukrainian military at the time still used the D-30 Howitzer artillery pieces (produced originally in the 1960s by the Soviet Union) and used an android application which was initially developed domestically within Ukraine by an officer of the 55th Artillery Brigade named Yaroslav Sherstuk. The application was used by around 9000 Ukrainian officers to efficiently calculate artillery trajectory and target the enemy positions. The X-agent was successfully infiltrated in the application by the Fancy Bear group and has facilitated reconnaissance against Ukrainian troops by displaying location and target calculation to the Russian troops. Reporting indicates that over 50% of the Ukrainian artillery forces have been lost over the 2 years of conflict and over 80% of D-30 howitzers, the highest percentage of loss of any other artillery pieces in Ukraine's arsenal (Meyers, 2019). This cyberattack is an example of how military and defense capacities can be compromised and impacted on the terrain amidst a conflict, and while this incident is rather specific it shows the existence of a vulnerability in defense systems. This case illustrates the argument made by Lt Col Lionel D. Alford of the US air force who concluded a rapport on cyber security by stating that "cyber operations have the potential to overcome any system controlled by software" (USAF, 2015).

The military potential of cyberattacks has been contextually witnessed throughout the conflict between Russia and Ukraine. Beyond the hacking of the artillery pieces that relate directly to combat, cyberattacks on Ukrainian infrastructure were witnessed at key moments of Russian offensives, these attacks will be discussed further chapters. A report by the Center for Security Studies of Zurich established this parallel between ground activities and the occurrences of cyberattacks on Ukrainian infrastructure, throughout the conflict cyber activities were at a low-level of intensity but peaked at critical moments of the conflict (Baezner, 2018). This further highlights the potential and importance of cyberattacks as a mean to acquire military superiority on the ground, and as a point of external pressure on the side of key military activities.

Military Applications of Cyber – Coordinated Military Intervention in Iran 2010

Energy-centered in origin, the Iranian nuclear history begun in the 1950s, the political climate evolved in the 1980s and leading up to 2002 when the National Council of Resistance of Iran revealed the existence of the Natanz enrichment complex (NTI, 2020). Between 2006 and 2008 a number of UN resolution demanded of Iran to stop its enrichment process, which Iran refused to cooperate with. The enrichment of uranium is done at three different levels, energy grade (3-4%), medical grade (20%), and military grade (90% and above), all three types can be achieved through similar enrichment processes. Iran pursued research and continued its enrichment activities to a point where the Atomic Energy Agency (IAEA) inspectors were not able to rule out a weapons program (NTI, 2020, Lindsay, 2013). The US long suspected Iran to seek to create military grade enriched uranium for the creation of nuclear weapons (NTI, 2020). In 2010, in collaboration with the Israeli government, the US government allegedly carried out a disruptive cyberattack on the Natanz enrichment facility – the attack would later be named "Stuxnet" after a component found in the infected computers by the forensic investigators (Lindsay, 2013).

The Stuxnet attack used a computer worm software, a form of self-replicating malware that once successfully implanted spreads throughout a given system. The malware remained hidden and controlled the centrifuges over a two-months period progressively sending false negative error reports and sabotaging the machines by degrading them – sending modified commands to the machines and altered reports to the operators (Lindsay, 2013). The Natanz facility has its own secured closed network, the Stuxnet worm was successfully integrated to a piece of hardware from a third-party manufacturer, which later was installed in the facility to spread (Lindsay, 2013).

Stuxnet is the first instance of a computer network attack to have caused physical damage across international boundaries, this complex tool was the result of a long, interconnected research program that was started under the Bush administration to be later picked up and executed by the Obama administration in 2010 (Lindsay, 2013). At the time Stuxnet was hailed as "the most technologically sophisticated malicious program developed for a targeted attack to date" (Clayton, 2010). In hindsight the cyberattack was a technological feat with a rather limited impact on the Iranian enrichment project, only delaying it by a couple of years. A much longer lasting impact

was the unveiling of the possibility to remotely impact physical infrastructures from abroad, bringing about a game-changing aspect to technological warfare.

Military Vulnerability - The Theoretical Vulnerabilities of Nuclear Weapon Systems

Nuclear weapon systems were conceived and built in a time where computer capabilities were in their infancy, back then little attention was given to the eventual rise of cyberattacks as a credible threat to the integrity of this system. Being the most direct and concrete threat in the realm of existential risk, nuclear weapon systems need to be evaluated in the context of cyber warfare. Having maintained their relevance as a threat to humanity since the cold war, nuclear weapon systems have been continuously upgraded to fit new kinds of digital technologies at every step of the launching sequence, whether in detection, communication, targeting, launch, or transport. The components of this launching sequence are known as the nuclear command, control, and communication (NC3) and increasingly uses digital technologies to enhance efficiency and reliability (Lindsay, 2019). Most response launch sequences depend on a dual detection method that requires confirmed strike incoming on two different modes of measurement (e.g. radar and satellite systems) this is called dual phenomenology, once established dual phenomenological detection places decision maker in control of retaliation decisions (Unal & Lewis, 2018). However, this system relies on a complex chain of events and the successful transmission of data and information, which is the most vulnerable point of a system when faced with a cyberattack (Hurson, 2015).

Cyber vulnerabilities in the nuclear weapon system could take multiple form at various stages of the deterrence sequence. Early warning and satellite radars could be tempered with either with spoofing (indue a false positive launch detection) or with blinding (indue a false negative launch detection) (Lindsay, 2019; Unal & Lewis, 2018). A cyberattack at the level of intelligence and assessment systems could impact communication by engineering confusion through flooding attacks, false flagging, and jamming of the data-reliant processes of NC3, this could lead to misattribution, threat inflation, or errors in decision making (Lindsay, 2019). The communication network itself could be breached by falsifying identity, authentication, or confidentiality which could result in targeting error or unauthorized launch (Lindsay, 2019). These key vulnerabilities

of the nuclear weapon system are caused by data breaches, the corruption or insertion of false data into the system that could lead to a breach in the NC3 and could realistically provoke a launch. Design vulnerabilities may also be introduced in the supply chain of nuclear weapons systems, as most nuclear-abled states rely on private sector contractors. Compromised source code from the private company could be integrated to a nuclear weapon system and corrupt its reliability, this in turn could result in an overconfident reliance on the stable functioning of the system by decision makers may lead to the issuing of an order without sufficient information (Unal & Lewis, 2018).

These cyber vulnerability scenarios have not materialized in practice, but according to the expert opinion exposed above, there are concrete vulnerabilities that could realistically lead to the inadvertent launch of a nuclear weapon. There is some concern that these cyber-NC3 mechanisms do raise the marginal risk of nuclear war, thereby making a highly unlikely event slightly more likely (Lindsay, 2019). The entanglement of cyber and nuclear must be considered a plausible global catastrophic risk scenario and as Unal and Leis (2018) point out: at best, cyber insecurity in nuclear weapons systems is likely to undermine trust and confidence in military capabilities and in the nuclear weapons infrastructure; at worst, cyberattacks could lead to deliberate misinformation and the inadvertent launch of nuclear weapons.

These revelations are a significant concern, but contextualized to the contemporary nuclear tensions, the cyber vulnerabilities in nuclear weapon systems add a significant level of uncertainty to an already catastrophic standoff (Bulletin of the Atomic Scientists, 2021). Considering the 2020 Doomsday Clock statement by the Bulletin of the atomic scientist we would find ourselves in a nuclear tension higher than what was experienced during the cold war, cyberwarfare is yet another unknown added to this nuclear equation.

Military Critical systems

Military critical systems, in both offensive and defensive contexts, have concrete vulnerabilities that can be exploited in cyberspace. The role of the military in society is predominantly a defensive one, that in of itself is a core critical function that is actively challenged in cyberspace. Standing militaries have become partly obsolete in cyberspace, the Iranian army could have realistically

done little to defend the Nantanz nuclear enrichment facility from a cyberattack. Cyberspace, digitalization, and the interconnectivity of infrastructures offers a convenient workaround the defensive notion of a physical army, forcing nations to rethink the concept of national defense. The nature of cyberspace is completely challenging the notion of a defendable sovereign space, the lack of borders and defined frontiers make it impossible to effectively protect. This is especially true when the digitalization of critical infrastructures exposes key pressure points in cyberspace, a realm that is incomprehensively hard to defend. It has been demonstrated that militaries around the world rely on digital technology for ground operations, the exposition of the French Orion Exercise and the overall integration of digital systems in military operations highlight the current evolution of modern military. The successful hack of the Ukrainian artillery targeting software is a concrete example of how digitalization can become a vulnerability on the field. Most states have begun to or have already established cyberspace as a realm of operation, the notion of offensive cyber capabilities has been adopted by most militaries around the world and we are seeing it becoming the new norm for military operations. In direct relation to existential risk the vulnerabilities of nuclear weapon systems exposed by Lindsay, Unal, and Lewis raise an important vulnerability that could if exploited truly be catastrophic.

Critical Infrastructure

Critical Infrastructure – Cyber-Physical System

In a report by the President's Commission on Critical Infrastructure Protection infrastructure was defined as “a network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services” (PCCIP, 1997). These systems include telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services (PCCIP, 1997). France has integrated the notion of critical infrastructure to their Code of defense (code de la défense) by creating the administrative label of “vital operators” (opérateurs d'importance vitale). The label of critical infrastructure is granted to the public or private organization that operates systems without which the war or economic potential, security or survival capacity of the nation would be significantly impaired

(code de la défense article L1332-1 à L1332-6). Upholding operational security is endowed to the operator itself under a specific set of rules laid out in the code.

Critical infrastructure used to be solely made of physical entities, controlled on site with mechanical systems that were operated in their entirety by workers. The critical infrastructure systems have progressively digitalized to meet the increased demand for basic services and evolving performance requirements becoming cyber-physical systems (CPSs), dependent on data, computer processing power, and embedded intelligent systems (Woodart et al, 2015). Nowadays the vast majority of critical infrastructure systems are controlled and monitored with Industrial Control Systems (ICSs) and/or Supervisory Control and Data Acquisition (SCADA) systems. Information and communication technologies have been integrated to critical infrastructures, this digitalization process both improved efficiency and allowed for the formation of an interconnected network that gave operators a more holistic point of view on how to run infrastructures. Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies (Rinaldi et al., 2001). Examples of these complex CPSs include smart power grids, intelligent water distribution networks, smart transportation systems, and cyber-enabled manufacturing systems. These digital improvements in the operation of infrastructure are heavily dependent on real time data collection to calculate optimal control settings (Woodart et al, 2015). There are many ways that this balance of data usage can be altered mainly through the corruption of data processed by the system, this corruption can be the result of a deliberate or nondeliberate actions. The nondeliberate creation of erroneous data refer to human errors or faulty programming, for the sake of this paper only deliberate corruption of data will be assessed. Deliberate creation of erroneous or corrupted data refers to a cyberattack on an infrastructure system that remotely compromise the confidentiality, integrity, or availability of data in the system these include denial of service and malware designed to disrupt a control system (Woodart et al, 2015). Cyber-physical infrastructure systems have multiple built-in fail-safe mechanisms that can detect if the system is being tempered with and theoretically prevent cyber-attacks from occurring. False data injection attacks are a type of cyberattack that have been specifically designed for bypassing these fail-safe mechanisms by feeding the system a steady stream of false negative reports while changing the physical components of the infrastructural system, as such, the operator's system remains unalarmed and the cyberattack takes place without being detectable (Liu, 2011). False data injection attacks are

limited by some physical constraints but have the potential to open concrete attack vectors that if achieved can deeply impact infrastructures and bypass existing defensive measures (Liu, 2011). Data corruption is achievable in a plethora of ways, paired with the increasing complexity of systems, and the possibility of human error, making critical infrastructure systems vulnerable targets for cyberattacks by nature.

Critical Infrastructure Interdependency – The Smart Electrical Grid

Infrastructural interdependency adds another layer of vulnerability to modern cyber physical critical systems. The digital technology that regulates and operates modern infrastructures depends on a stable and consistent flow of electricity, along with being a critical infrastructure in of itself, the electrical grid is powering other critical infrastructures (Rinaldi et al., 2001). Telecommunication, transportation, air travel, water, gas, oil, and finances are all to different degrees depending on the electrical grid, this makes electrical production a prime target for disruptive cyberattacks. In turn the electrical infrastructure requires oil, gas, or transport of materials to produce and provide electricity, this interdependent system vastly improves efficiency but gathers all sensitive pressure points under one roof, making the system efficient but fragile.

In December 2015, a synchronized and coordinated cyber-attack compromised three Ukrainian regional electric power distribution companies, resulting in power outages affecting hundreds of thousands of citizens for several hours (Liang et al., 2017). Three distinct attacks vectors were set up to culminate in the successful disruption of the electrical grid: the Black Energy 3 malware was implanted remotely via an email phishing attack, a telephonic denial of service overwhelmed the call centers blocking the reports of failure, and the “killdisk” malware was implanted to delete records on workstations and lengthen the recovery time (Liang et al., 2017). The success of this shutdown was ensured by the disruption of the electrical backup systems which would have normally ensured supply in the event of a shutdown. The Black Energy malware had been discovered in 2014 by an American cyber security firm, the software was found to be specifically designed to create an access bridge between digital and physical infrastructures (NBC news, 2019). These security compromises led to the hijack of the Supervisory Control and Data Acquisition (SCADA) network, enabling attackers to remotely open the system breakers and disrupt power supply. Once breached the electric grid system was open for remote manipulation,

the Human Machine Interface (HMI) of the supervisory control system was overtaken entirely by the hackers, workers on site recollected seeing the mouse control of the panel acting on its own shutting down the circuit brakers one by one in front of their eyes (New America, 2019). This was achieved through the obtention of login credentials via previously infected devices and communication interceptions, the SCADA network was using basic non-encrypted security and with the appropriate knowledge the attackers successfully entered the system, the same breach was later used to wipe data and information and delay restoration efforts (Liang, 2017).

There were clear signs that the 2015 Ukrainian blackout was achieved by a successfully carried out false data injection attack, this is argued by Liang et al (2017) and is supported by the joint rapport published by the SANS Industrial Control System and the Electricity Information Sharing and Analysis Centre by Lee et al. (2016) in which they concluded that "Nothing about the attack in Ukraine was inherently specific to Ukrainian infrastructure. The impact of a similar attack may be different in other nations, but the attack methodology, tactics, techniques, and procedures observed are employable in infrastructures around the world." The paper that introduced the concept of false data injection attack (Liu, 2011) concluded at the time that "despite the theoretical capability of these attacks (FDIAs), we also pointed out that such attacks are strictly limited by real-world constraints, and do not pose immediate threats to our power grids."

In hindsight the 2015 Ukrainian blackout was not a catastrophic event, the power outage impacted about 200,000 citizens for a time spanning from 1 to 6 hours, cutting altogether the supply of 73 MWh of electricity or 0.015% of the total daily electricity consumption in the Ukraine. The notable aspects of this cyberattack relate to the insight of the hackers, their ability to implant data and coordinate the attack on 3 different targets of the Ukrainian power grid. The killdisk malware erased most traces that could have led investigators to identifying the origins of the attack, but the Ukrainian government has been adamant about blaming Russia (Lee, 2016). In 2020 there was an attempt by the US department of Justice to indicted six Russian Main Intelligence Directorate (GRU) officers for their involvement in hacking incidents including the 2015 and 2016 attacks on Ukrainian critical infrastructure (DoJ, 2020).

In October 2020, Mumbai, the financial center of India suffered a massive electrical blackout. The blackout occurred as a result of a cyberattack on the city's electrical grid, which occurred during the border dispute between India and China in late 2020, reports in March 2021

showed evidence of cyberattack. The Indian authorities accused China, but all allegations have been rejected by Chinese officials (Stringer & Lee, 2021). Millions were left without power, trains were stranded and online college exams and mobile telephone services collapsed after a grid failure that affected all of Mumbai and lasted for more than 12 hours in some parts of the city (Reuters, 2021). Adding to existing vulnerabilities of power grids, producers and distributors have also often been reluctant to spend on protecting themselves against low-probability attacks (Stringer & Lee, 2021).

Critical Infrastructure Vulnerability – Teachings from the Aurora Test

In March 2007, an Idaho National Laboratory experiment supervised by cybersecurity pioneer Michael Assante exposed that cyberattacks on electrical infrastructure could be much more than just disruptive. The test of a hacking tool on an isolated electrical diesel generator ran a 30 lines long code on the operating system of the machine forcing it to desync and resync to the grid while running, blowing up the generator within minutes (Greenberg, 2019). This code file could fit on a .gif file, no bigger than a low-resolution photo and once executed, successfully brought down a 27-ton generator. The experiment took on the name Aurora Vulnerability Test and proved without a doubt that hackers who attacked an electric facility could go beyond temporary disruption of the victim's operations: they could damage its most critical equipment beyond repair (Greenberg, 2019). This highlighted a systemic flaw in the outdated American electrical grid which was implemented in the late 1800s with principal goal the distribution of electricity to as wide a crowd as possible, and on consumption standards on par with the technology of the time. Many of the current US's facilities have not been updated since the 1960s, and loose power three times more often than they did 50 years ago.

In 2020, following the proof of concept and the conclusions drawn from the Aurora test, a $3 Million, 250 Tons power transformer manufactured in China was seized and sent to the Sandia National Labs in New Mexico. The purpose of this seizure remained unclear until half a year later when the Trump administration issued an executive order "Securing the United States Bulk Power System" aiming to keep critical equipment supplied by foreign adversaries out of the nation's power grid due to supposed supply chain security threats (Executive Office of the President, 2020).

The executive Order implicitly targeted China suggesting that backdoor malware was installed in the overseas components designed to be installed in the US electrical infrastructure finding that "foreign adversaries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system" (EO #13920). While no links have been officially established the chain of event has led journalists to speculate on the nature of the seizure of the Chinese transformer and raises the question of national control of critical infrastructure from supply chain attacks (Smith, 2020).

Broad Critical Infrastructure Vulnerabilities – Notpetya Ukraine 2017

The story behind the Notpetya malware is as intricate as it is interesting, journalist Andy Greenberg extensively covered the topic as the attack unfolded in 2017 in his book "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" published in 2020. Named after the monster from the sci-fi novel "Dune" Sandworm is the name of a hacker group connected to the Russia GRU and the FancyBear group, they are at the origin of the Notpetya ransomware which stroke Ukraine in 2017. Arguably the most advanced hacking tool in history the Notpetya cyberattack had rippling effect throughout the Ukrainian infrastructure and impacted multiple aspects of society, in Ukraine and abroad.

MeDoc is an accounting and tax filing software ran by the small tech company called Linkos Group, it is used by 90% of the domestic firms in Ukraine in both private and public sectors. The Sandworm hacker group successfully infiltrated the Linkos Group's server responsible for sending out updates of the MeDoc software, from there every computer that updated the accounting software became infected (Greenberg, 2020). In late June 2017, the infection had begun, it became apparent on the 28th of June (Ukraine's constitution day) the first victim was the Oschadbank who reported early signs of ransomware. Ransomware is a classic malware that locks a device's data in exchange for a ransom, this specific ransomware appeared to be a version of the wannacry ransomware, but as Greenberg (2020) explored, the malware was a smokescreen for the real malware infiltration: Notpetya. The data encryption malware ran through the device's data, permanently locked that data out for the users (results on par with permanent deletion) and proceeded to take over the Windows management tool allowing it to spread through the network

to another computer where it proceeds to repeat the infection, lockdown, deletion, spread sequence (Greenberg, 2020).

The malware spread uncontrollably in the days and weeks following the attack, the blunt of the impact was felt by Ukraine. The cleaning facilities of the Chernobyl nuclear power plant site were locked and unable to communicate or operate properly, the Chernobyl site went dark with as its last message "To all staff members, immediately turn off computers and unplug network cables. Await further instructions" (Greenberg, 2020). Some were able to react quickly enough and disconnect their networks to avoid infection, the Ukrainian health minister was warned ahead enough to do so, but most Ukrainian federal agencies were impacted by the malware "The government was dead," summarizes the Ukrainian minister of infrastructure Volodymyr Omelyan. The Ukrainian postal service, in charge of post, newspaper distribution, and perhaps more importantly money transfers and pension payments, went offline too late and had 70% of its data erased permanently, leaving the system crippled for months. The credit card system and a vast portion of Ukrainian banks suffered the same fate, rendering credit card transaction unusable for most purposes. At least four hospitals in Kiev were impacted, every piece of equipment that ran windows OS was disabled, from the patient's data, records, and test results that were hosted on the hospital's servers to the GPS tracking system used to locate and dispatch hospital ambulance units, all were locked on the ransomware black screen while data was being erased. In sum, by the end of June 27, NotPetya had struck at least four hospitals in Kiev alone, along with two airports, more than twenty-two Ukrainian banks, ATMs, and card payment systems, six power companies, and practically the entire federal government – an estimated 300 companies were hit and records have indicated that about 10% of all computers in the country were wiped (Greenberg, 2020).

Broad Critical Infrastructure Vulnerabilities – Notpetya International 2017

The NotPetya worm did not stop to Ukraine, the Danish shipping company Mærsk had an office in Odessa near the black sea, there an accountant had installed the MeDoc software on only one of their computers, which was enough to give the worm a foothold in the company. The headquarters in Copenhagen went dark on the same day, and soon after the Mærsk shipping terminals abroad started failing, the impact this time was much more physical, hundreds of thousands of tons of shipment were waiting to be loaded on thousands of dispatch trucks. The problem was that this

digital choreography depended on Mærsk's data to match containers with trucks and destinations, shipping stopped for two weeks before the digital system was re-established (Greenberg, 2020). Thousands of tons of shipment were delayed, the company announced an estimated loss of 200 to 300 million USD due to the Notpetya cyberattack (Lord, 2020).

The worm spread widely and indiscriminately from device to device, if it was connected in some way to an infected device, the worm would find a way to spread to it. American multinational delivery services company FedEx was also impacted, the worm spread through their services and in a similar fashion locked and deleted key operational data from their operating systems. Hundreds of companies and organizations around the world found themselves victims of the NotPetya worm, with traces of the cyberattack lingering throughout the years and trails of the worm still found in devices today. In their 2019 annual report the firm reported having spent approximately $400 million in remediation and related expenses (FedEx, 2019). American multinational pharmaceutical company Merck & co were also hit by the worm and reported cost of mediation to $670 million (Nash et al., 2018).

Fuel Distribution – Colonial Pipeline 2021

In May 2021, Colonial Pipeline, the largest pipeline company for refined oil products in the U.S., announced that it had been the victim of a cyberattack that locked its control system behind a ransomware wall. The hack completely stopped operation and distribution of fuel for a week, prompting panic buying and gasoline shortages throughout the East Coast (Satter, 2021). The attack took place in early May and after a successful intrusion the operating system and data of the company were encrypted with the DarkSide ransomware. The perpetrators are from an eastern-European hacker group called DarkSide, affiliated with Ukrainian, Russian, Belarussian, and Georgian hackers it is a prominent group that has successfully executed multiple large-scale cyberattacks on private corporations, mainly asking for ransom in crypto currency (Dowd, 2021). The hacker group is known to operate from eastern Europe and to be constituted of eastern European hackers, but investigators are confident that the group is not government sponsored.

The attack was the first from the group to impact infrastructure, the damage was minimal, most of the data was recovered and operations resumed after Colonial reportedly paid the Darkside a ransom of nearly $5 million in bitcoin (Dowd, 2021). The supply of fuel recovered over the two days following the payment, in the week of the shutdown American rushed the gas pumps and panic buying at every gas station ensued with harrowing accounts of people filling up plastic bags with gasoline which accelerated the shortages. The damages were limited, and the company managed to take some of the operating systems offline quickly before the malware spread to them, in spite of that the supply was halted. What is worth considering is that every airport along the south eastern and eastern coasts of the US are dependent on the fuel supply from the Colonial Pipeline. Joe Biden issued a statement in which he emphasized the non-state origin of the attack and called upon citizens to remain patient with the return to normalcy, he also highlighted a critical aspect of the relationship between government and privately-owned infrastructure "the bottom line is that I cannot dictate that the private companies do certain things relative to cyber security" (NBC News, 2021). Biden also mentioned the establishment of a compromise-based discussion between the federal state and the private company to ensure recovery, executive orders temporarily lifted restrictions and governmental support was provided to re-establish the supply of fuel. This cyberattack brought up the question of the relation between a government and its privately owned infrastructures and highlighted a key flaw of this relation in the context of the attack: government intervention in crisis situation.

Critical system – Critical Infrastructure

Critical infrastructure is perhaps the most direct point of pressure in a society, the reliance of citizens on consistent supply of everyday appliances like water, electricity, gas, fuel, heat, and the overall interconnectedness of these systems makes critical infrastructure a prime target for cyberattacks. The unprecedented impact of the NotPetya attack shook the Ukrainian infrastructure to its core, entire ministries went offline, vital bureaucratic tasks, credit card and banking infrastructure, public services, hospitals, and various computer systems that ran Windows OS were taken down.

While not expanded upon in this chapter, the reality for hospitals and healthcare as a critical system has worsened during the COVID 19 pandemic. The data wipes that impacted Ukrainian

hospital during the notpetya attack is just a glimpse of what the healthcare field has experienced. Hospitals are particularly prone to ransomware attacks and are often easy prey due to a lack of cybersecurity in their systems. These attacks have only worsened during the Covid19 pandemic as healthcare capacities were particularly stretched out and vulnerable, with increase in severity and frequency, international and national bodies have stressed the importance of increasing cybersecurity capabilities of hospitals (Muthuppalaniappan & Stevenson, 2020).

This section showcased the extent to which critical infrastructures are vulnerable to cyberattacks. Power grids are increasingly vulnerable to cyberattacks, and the number of attacks on electrical grids in increasing (CSER, 2021). As the central node to other critical infrastructure, the electrical systems around the world are facing increased demand in terms of energy production, and this increased reliance in turn amps up the vital importance of these systems to society. The Aurora Tests have showcased a new vulnerability that can be either delivered to or inherently implanted in critical infrastructure systems, expanding the number of possible attack vectors in electrical systems. The notpetya attack also showcased how vulnerable international shipping infrastructures are, the impact on Mærsk was devastating and halted operation for weeks, other private companies suffered similar impacts and dealt with the onerous aftermath of the attack.

Global spread mechanisms

There are a multitude of cracks and vulnerabilities that allow for malicious actors to constitute concrete attack vectors for carrying out a successful cyberattack on contemporary digital systems. This section draws from the previous cases and academic arguments to identify the ways in which a cyberattack can be carried out and the mechanisms through which it can spread globally.

Following Libicki's (2015) argument with increased complexity in critical systems, comes a heightened tendency for human error which can be manifested in different ways throughout modern digital systems. Short and simple credentials can offer an easy access to any malicious actor, multiple factors identification or compromised passwords are all aspects that constitute basic cyber hygiene but are often the most straightforward point of access for hackers and criminals. Weak cybersecurity or poor encryption can constitute the same level of threat, encryption has not

yet entered the norm for basic digital hygiene. However, none of these are miracle software solutions and as the solarwind hack demonstrated, no system is totally infallible and human error offers an easy breach into the most sophisticated cybersecurity systems (Banga, 2021).

The attack itself can take multiple forms, ranging in complexity from simple brute force to an elaborate attack. Brute force attacks are a relentless trial and error method to access encrypted data or guess a password, similar to a burglar trying to crack a lock. There are some basic counter measures to brute force attacks that are integrated into most systems. However, the cover of anonymity and modern computing methods allow hackers to attack defenses indefinitely without facing reduced chances or consequences. Distributed Denial of Service (DDoS) is a type of flooding attack that overwhelms a server or device with a disruptive goal in mind, essentially making the device, website, or service inaccessible or causing it to crash. The 2007 cyberattack against Estonia is an example of a DDoS attack. Zero-Day Vulnerability Attacks abuse intrinsic flaws of a system that are unknown to the defender up until the breach occurs; this is an inherent flaw of digital systems. Ransomware is a tool used to lock data, access, or control of a device from its user by encrypting data on the device. To recover access the user must pay a ransom, usually in crypto currency, a form of currency that is harder to trace once distributed. Examples of ransomware attacks include the initial phase of the NotPetya attack, or the Colonial Pipeline attack of 2021; ransomware is a commonly used tool by hacker groups like the Fancy Bear or Sandworm. Phishing is a form of cyberattack that targets a trusted source of the user like email, phone number, or text message to trick the user into opening a link between the hacker and a trusted device. Phishing is a frequently used tool to bypass two factor authentication, it is also a tool that successfully abuses the human component of systems by luring a user into sharing passwords, credentials, or personally identifiable information, the first phase of the 2015 Ukrainian blackout included a phishing attack. Computer worms are a form of malware that is designed to spread from one device to another, it does so by self-replicating and spreading through networks. The Not Petya worm is an example of a computer worm, it was extensively used throughout Ukraine and impacted hundreds of systems internationally between 2017 and 2019.

New software is rarely designed from scratch, programmers often rely on existing repositories of algorithms, so they don't have to “reinvent the wheel” when building complex systems. Repositories, such as JavaScript's Node Package Manager, are used extensively by

developers worldwide and boast millions of lines of code's worth of content. In February 2021 a security researcher detailed how he was able to hack into systems belonging to Apple, Microsoft, PayPal, and other major tech companies in a novel software supply chain attack (Haworth, 2021). This was achieved through dependency confusion or integrating strands of readily available codes with malicious lines of code that once picked up and implemented by programmers become an infected piece of a puzzle. Using this method, the security researcher was able to exploit this vulnerability to breach the internal systems of the above mentioned organizations as well as Shopify, Netflix, Yelp, Tesla, and Uber (Haworth, 2021). This is another way for malicious code to make its way to a system or device, regardless of whether they are connected to the internet after deployment.

An anecdotal type of attack has been revealed to be veridic by a team of researchers at the University of Illinois and Michigan, "USB thumb stick drops" attacks that consist of dropping an infected USB stick near a military base and counting on human curiosity to plug it in a computer connected to the targeted system. The team of researchers investigated the issue based on an anecdotal attack on an undisclosed US military base using a simple USB drop method, they concluded that that "users are initially acting altruistically, but their curiosity eclipses their altruism as they try to find contact information" with results varying from 45% to 98% of the USB drives were plugged in devices and successfully infected the participants (Tischer, et al., 2016).

There are multiple ways to defend against these methods, practices like cyber hygiene and cybersecurity methods like Proof of Concept exploits can protect an organization or system from these attacks. As discussed throughout the theory section, cyber security entities are in a constant tug of war with malicious hackers that consistently and constantly find new vectors of attack in contemporary digitalized systems.

Global spread mechanism - SCADA systems

Irmak & Erkerk (2018) deepen the identification of global spread mechanisms by identifying cyberattack vectors that are specific to critical infrastructures and their Supervisory Control and Data Acquisition (SCADA) systems. Attacks targeting hardware are particularly efficient for closed networks (not connected to the internet or any external networks) and are often carried out

as a hardware implantation via third party company. This was the alleged procedure of the 2010 Stuxnet cyberattack on the Natanz nuclear facility, the malware was installed on an independent third party-issued hardware that once installed in the facility spoofed the SCADA system readings while damaging the centrifuges of the cite. Hardware attacks can also be conducted on site, where code or malware could be directly injected in the facility systems (Irmak & Erkek, 2018).

Attacks targeting software are much more common and can be executed remotely ensuring a certain level of anonymity and reducing detection risks for malicious actors. A US Department of Homeland Security developed the National SCADA Test Bed program which analyses and identifies existing security flaws in SCADA source code and software design (2011). The software identified three common vulnerabilities: input validation, authentication, and access control; all of which were found in source codes of SCADA systems of critical infrastructures (USHS, 2011). One key limitation is that source code updates of SCADA systems is difficult to roll out and largely depend on the (often private) operator of the critical infrastructure, since software update could engender technical complications most SCADA systems might in fact be outdated (USHS, 2011; Irmak & Erkek, 2018). Buffer overflow is a common input validation vulnerability in SCADA systems, which occurs when the software writes more data to the memory than the space allocated causing the program to run outside of normal functions in a scenario prone to breaches (Irmak& Erkek, 2018).

Lastly, attacks targeting communication systems can disrupt SCADA system efficiency and can impact operation, as mentioned in the chapter on critical infrastructure, many critical infrastructures depend on real time data to regulate flows and service delivery, this is especially true of electrical grids and pipelines. A disruption in data communication of just a millisecond can create a halt in operation, this can be managed with real-time data inspection and security test, which not all SCADA systems can accommodate in tandem with operation (Irmak& Erkek, 2018).

In the context of cyberspace, anthropogenic networks like the internet, communication networks, or information and communication technologies are the main global spread mechanism. Replicators thus far have mainly been individual hackers, but the spread of the NotPetya Worm drastically expanded the realm of possibility in terms of spread of cyberattacks, essentially cascading through connected systems at the speed of digital communication.

Discussion

The environmental scanning analysis has explored various instances of cyberattack in an attempt to depict the range of possibilities in cyberspace. Identifying critical systems and global spread mechanism from the classification of global catastrophic risks methodology. The combination of these two allows us to already infer on the extent to which cyberwarfare can be considered a global catastrophic risk scenario. However, holistic risk management must take into account the human element that moderate GCR through prevention and mitigation efforts (Avin et al, 2018). This section will take the cases explored in the analysis and use them in a discussion that aims at identifying the prevention and mitigation failures of catastrophic cyberattacks.

Normative Prioritization.

Throughout the research on existential risk and GCR the threat of artificial intelligence is consistently presented as the next technological risk that humanity will have to deal with. Bolstered by the cautionary speeches of famous personalities like Elon Musk or Stephen Hawkins, both calling out the tremendous potential of artificial intelligence as the next threat to humanity, the theoretical and unproven threat posed by AI seems to have overshadowed the reality that is unfolding in cyberspace. Martin Rees (2004) wrote "our final century" where he considers "rogue nano-machines that replicate catastrophically" as a credible technological threat to humanity but does not account for potential impact of cyberwarfare. Both the 2018 and 2020 Global Catastrophic Risks reports from the Global Challenge Foundation categorize Artificial intelligence as the next technological challenge that humanity will face (GCF, 2018; GCF, 2020). The 2018 report indicates that Artificial Intelligence might be decades away and might use vectors along the lines of warfare, finance, cybersecurity, and political institutions, privacy, and employment to impact society. This speaks to one of the normative limitations in preventing a cyber-enabled global catastrophic risk scenario: the lack of prioritization in academic and organizational literature as to which technological threats should be prioritized first.

Australian roboticist Rodney Brooks wrote the "7 deadly sins of AI prediction" published in the MIT Technology Review magazine in 2017. There he laid out 7 arguments that explore how wrong predictions about AI can impact the technological and political landscapes negatively. "We are surrounded by hysteria about the future of artificial intelligence and robotics—hysteria about how powerful they will become, how quickly, and what they will do to jobs." (Brooks, 2017). He argues that despite the tremendous advances in the field of computing and AI the complexity of the task at hand (creating human level consciousness) is mystified and blown out of proportion as to what the threat really is (Brooks, 2017). Bostrom (2013) indicates that there seems to be a prioritization and/or overestimation of less probable risks (e.g. asteroid collision) and an underestimation of more imminent and probable technological risks. Considering the critical systems vulnerabilities explored in the analysis these are already attack vectors used to abuse vulnerabilities in the critical systems of society, the prioritization of the threat of artificial intelligence in the agendas only delay effective governance and the prioritization of the already demonstrated impact that cyberwarfare has.

This prioritization has a normative impact and tends to divert attention away from the real extent of the threat posed by cyber warfare. Furthermore, the threat of a cybercrime tends to capture the attention of citizens much more than the threat of cyberwarfare, this is bound to a form of cognitive bias that makes individual relate to individual-scale threats much more than grander threat. As such, a lot of the political and societal attention is placed on micro-level threats (bank account theft, identity theft, phishing, spam, spyware) on the individual and tends to encompass what constitutes a cyberattack in the imaginary of people. This is seen at the individual level with the explosion of protection software especially VPN companies (Nord VPN, Dash lane, express VPN), and at the political level with the often flawed understanding of politicians vis-à-vis the technological reality of cyber (IPU, 2021). This lack of prioritization can pose an hinderance to the mitigation and prevention of catastrophic cyberwarfare, whether by underestimating it because of a cognitive bias, the lack of social and political awareness due to the non-normative salience of the issue, or plain misunderstanding.

The lack of clarity & attribution

There is this unanimous lack of common understanding of what constitutes cyberspace, both as a medium for human interactions but also as to what constitutes a cyberattack; paired with the problem of attribution this epistemic hurdle makes for one of the biggest preventions and mitigations failure. A solid, fact-grounded, commonly understood notion is key for designing mitigation, preparation, and response measures. There have been some definitions established, notably by the US CYBERCOM which defined it from a military perspective as a field of operation, the United Nations defines it along the lines of peace and security, human rights and sustainable development, the International Telecommunication Union (ITU) focuses on the technological aspect of the ITCs forming cyberspace, but the lack of clarity is a strong hindrance to common progress in securing and sustaining peaceful usage of cyberspace.

The concept of a concise definition is sometimes not achieved within a state itself, back in 2013, Lieutenant Colonel Samuel P. Mowery of the United States Marine Corps argued that to respond appropriately to threats in the cyber domain, the U.S. government needs whole-of-government definitions to determine what acts constitute cybercrime, cyber warfare, and cyber terrorism (Mowery, 2013). Furthering this argument, American political scientist Peter Singer wrote about the U.S. military official's stance on cyberspace and cyberattacks and called out the US military and the press at large for associating cyber warfare with historical military events like the cold war, pearl harbor, or the Cuban missile crisis. Gaps in understanding and dated conceptualization leading officials to treat cyberspace as a field of operation on par with the traditional physical field (Singer, 2014). This can lead political and civil and military leaders to be caught off guard when facing a cyberattack or a situation in cyberspace. In a seminar at "Talks at Google" (2014), he mentioned how military officers file in "cyberattacks" under the same category regardless of whether they are an insignificant prank call made by teenagers, or a cyberattack on infrastructure by a nation state, leading people to misinterpret the nature of cyberthreats in a "boy who cried wolf" scenario. These impact the perception of the public and of the political spheres and contributes to the lack of clarity that is so key for effective decision making, prevention, and mitigation.

Attribution is the other key aspect of cyberspace that heavily limits mitigation and prevention efforts. As explained in the theory section attribution of cyberattacks is by nature difficult if not impossible, throughout the cases studied attribution was a constant problem, keeping governments from addressing the post-attack recovery, and almost entirely preventing prosecution. The nature of cyberspace grants immunity to military weaker actors an asymmetric advantage, offense if becoming easier while defence is growing harder, and the difficulty of attributing the attacker's identity undermines deterrence (Lindsay, 2013). However, furthering Lindsay's argument, not only is the asymmetric nature of cyberspace granting heightened potential to small actors, but in the context of accountability and respect of Human Rights and International Humanitarian Law, it gives aggressive nation states a window of action and a plausible deniability "get out of jail free card" while attacking other nation states. This is, as will be argued further in the discussion, arguably the case of Russia, who has been extensively expanding and testing its offensive cyber capabilities on states like Russia, Estonia, France, or the US.

One extraordinary prosecution was carried out by the Department of Justice of the United States of America (DoJ) in October 2020, the investigation of cyberattacks against (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games brought the DoJ to charge six Russian GRU officers with connection to worldwide deployment of destructive malware and other disruptive actions in cyberspace (DoJ, 2020). The defendants were all officers of unit 74455 of the Russian GRU, linked with the notpetya attacks, the Ukraine attacks between 2013 and 2017, and other attacks like the Pyongyang Winter Olympics hacks and cyberattacks on the 2017 French elections (DoJ, 2020). These officers were successfully identified after credible information was posted on a website relating to the Sandworm group where the officers in questions claimed the attack and were bolstered for the cyber accomplishment (DoJ, 2020). However, it is important to remember that the officer will most likely never be trialled and/or sentenced since there are no extradition treaties between US and Russia, and the defendants are unlikely to ever find themselves on US soil. Furthermore, it could be argued that the DoJ trial against Russian unit 74455 has more of a façade to publicly appear tough on Russian cyberattacks and stand to the side of the impacted US allies, rather than an actual attempt at bringing about justice. The division within the US bureaucratic justice system and the lack of willingness to pursue a juridical and international conflict with Russia over poorly sourced and

alleged cyberattacks. In April 2021, the Biden administration issued economic sanction against Russia, furthering the long line of already in place sanctions set up from the 2014 annexation of Crimea, along with a diplomatic sanction that expelled 10 Russian diplomats (BBC, 2021). Both sanctions were seen as an attempt to walk a tight line between imposing a consequential enough cost to the alleged Solarwind cyberattacks and other "unacceptable behaviours of Moscow" in cyberspace, while maintaining a certain level of diplomatic relations.

Establishing clarity in cyberspace is a vital to ensure stability in interactions between nations, legal ambiguity in cyberspace might be alluring for some states in the short term, but it is decidedly a poor operational or strategic choice (McLaughlin & Schmitt, 2017). The application of International Humanitarian Law, a respect of Human Rights, and a general sustainable peace are clear targets to achieve in cyberspace for international institution. However, the application of laws designed for the physical world with direct human interactions, physical borders, and a generally respected sense of sovereignty, are hardly applicable online for they lack these specific prerequisite axioms.

Cyber as the new military norm

The use of offensive cyber capabilities in a military context has been discussed throughout the analysis section. Most countries have adopted cyberspace as the fourth frontier of warfare alongside with the classical fields of air, sea, and land. NATO and the US both have publicly announced their advances in cyber technologies in the military context and some have already tested them. Returning to the argument made by Robert J. Art (1980) and the expansion of the theory of offensive military capabilities into cyber by Lin and Smeets (2018), the role of deterrence in cyberspace is downgraded due to the nature of the medium of operation. Accordingly, efficient deterrence in cyberspace is left almost exclusively to reputation and credibility which is itself built through the post-deployment results. This seems to apply to the stance that Russia has adopted in cyberspace, their constant probing of these defenses of neighboring countries and cyber operations conducted abroad to showcase a certain desire to build up credibility as a cyber deterrence nation.

While the Trump administration effectively altered the processes of accountability that restrict the US military while undertaking cyber operations, there is still a certain level of liability on the part of the US cybercom vis-à-vis the US congress. In essence the US-led cyberoperation

are bound to some extend by institutionally-enforced accountability, this is not the case of every other cyber-abled nation. Russia, mainly through the actions of the GRU, operates without much accountability in cyberspace, their cyber operation over Ukraine showcased a level of recklessness that rippled through Europe and much of the world. The technology used by groups like Fancy Bear, unity 774455, Sandworm, and the GRU at large have showcased level of depth for cyber attacks that are setting a new precedent for the field of cybersecurity. Their attacks on Ukraine's critical infrastructure, government, military, and communication systems, the first nation-wide attack on Estonia, and the Solarwind attacks have established Russia as more than able to conduct operations in cyberspace securing its place as a force to be reckoned with, hence efficiently applying cyber deterrence. The actions of Russia in cyberspace impacted lives of citizens, have cost hundreds of institutions countless sums of money, and disrupted nations on scales rarely seen in the modern age. During a conference about the sandworm group at "Talks at Google" in 2019 Andy Greenberg and Peter Singer raised an interesting question: what if the damages caused by the NotPetya worm had instead been caused by a GRU special ops on the ground with a gun or explosive? The international response might have been vastly different.

Cyber operations do not occur in a vacuum, beyond establishing a stance as a credible cyber-abled nation Russia is expanding its offensive cyber capabilities and is concretely arming itself. Considering the Russian interventions in cyberspace, especially in Ukraine and Eastern Europe, an historical parallel can be drawn with the 1937 bombing of the Spanish city of Guernica. The civilian town of Guernica saw itself the first historical target of air raid bombings, it has been argued that the destruction of Guernica was of no strategic value in of itself, rather it is often considered a testing ground for the German blitzkrieg method that would see use throughout world war II (Manzanares, 1997). The international community at the time failed to speak out against the massacre of Guernica, famous Spanish artist Pablo Picasso immortalized the attack in one of his most famous piece "Guernica". The lack of outrage from the international community at the time, paired with the political context of the late 1930s allowed Germany to perfect its air raid capabilities. The same way Guernica was considered a target practice with no strategic value, many of the contemporary cyberattacks conducted by Russia have no inherent strategic value. Temporary disruption, data file corruption, and network intrusions can appear insignificant in a vacuum, for proof cyberattacks thus far have claimed no direct victims. However, analyzing these attacks solely on the merit of their direct impact is ignoring the possibility of long term military

application that are appearing at the horizon. Another detail to take into consideration is the room for error that could lead to escalation; as it has been shown cyberattacks are already consequential enough to be deemed a substantial threat, but the lack of agreement on what constitutes a cyberattack and the difficulties in attribution can realistically lead to a situation where a cyberattack could escalate into conflict. In 2019, NATO Secretary General Jens Stoltenberg published an official statement maintaining that "A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all" (Stoltenberg, 2019). Raising questions about the efficacy of the deterrence of article 5 in cyberspace, which was arguably not enough to dissuade malicious actors from attacking Estonia in 2007. Some would go as far as argue that the entire deterrence spectrum of NATO states, including article 5, and the US nuclear umbrella, were put in question by the cyberattacks on Estonia (Herzog, 2011).

Limitations of application of IHL

International Humanitarian Law (IHL) is a body of law that regulates and delimits, for humanitarian reasons, the effects of armed conflicts. The main purpose of IHL is to protect the persons who are not or no longer partaking in an armed conflict by restricting the methods of warfare. Note that International humanitarian law applies only to armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence (ICRC, 2004). Until now, most cyberattacks have occurred outside of the context of armed conflict. However, the expansion of military operation into civilian areas of society is a growing concern in the IHL community. Using offensive cyber capabilities as a targeted strike on infrastructure, hospitals, communication, or any of the previously mentioned fields that are well within the reach of cyberattacks, can allow a state to effectively pressure sensitive areas of a nation while bypassing traditional kinetic warfare (e.g. bombing).

The first attempt to bring cyberattacks under the jurisdiction of IHL was made by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in the publication of the Tallinn Manual, a non-binding study on how international law applies to cyber conflicts and cyber warfare. The publication was a collaborative effort that brought together experts in the field of international law and cyber warfare, the core effort of this gathering was to examine cyberwarfare in relation to the application of international laws. The Tallinn manual does not represent the views of NATO

or its allies, rather it is the endeavour of international experts to provide guidance to decision makers around the globe on topics of international law and cyberwarfare. While the Tallinn manual initially focused on cyberattacks between states in the context of an armed conflict, it was expanded in 2013 to treat the eventuality of a cyberattack during peacetime.

The key recommendation of the Tallinn Manual is centred around strengthened partnerships and due diligence. Due diligence is arguably the most important normative steppingstone towards safer and peaceful utilization of cyberspace. It is a non-binding requirement that demands of states to not use cyberspace as a pathway to infringe on IHL and to ensure with a reasonable degree of feasibility that their sovereign land is not used to carry out such attacks. The experts of the Tallinn Manual have explicitly highlighted this normative step as a much-needed collaborative step, but the concept is rather divisive step. Following the United Nations Group of Governmental Experts, most countries were in favour of admitting that they "should" adopt due diligence methods rather than stating that they "must" do so. The efficiency of such a step depends wholistically on universal application, which in the current climate seems unrealistic. However, due diligence in cyberspace appears to be a pre-requisite for a path forward to be carved, international law acknowledges that the right of sovereignty and the corresponding duty of due diligence must be in equilibrium (Shmitt, 2015). Under the current trend of technological progression, it is unclear how governments are expected to reasonably prevent their territory from being a launching ground for cyberattack without incurring unreasonable spending in monitoring activity on cyberspace.

The UN Group of Governmental Experts established had for aim the establishment of a norm for responsible state behavior in cyberspace. Their work spanned 6 subsequent groups (fifteen to twenty-five rotating UN members) with notable development in 2013 with the adoption of a consensus report outlining a set of ground norms for the governance of cyberspace and reaffirming that international law, state sovereignty, and human rights apply to cyberspace, forming the groundwork for other UN-related cyber-related discussion (Basu et al., 2021). The Open-Ended Working Group which is includes all member states is struggling to find an agreement between the US and its allies and states like Russia and China who want to steer the UN OEWG in a direction that aligns with their respective national interest. Definition of key terms like information sovereignty has also created controversy amongst member states with western

democracies opting for a more liberal stance while China argues for a definition that would not challenge its current restrictive media environment.

The limitation remains, most parties agree that IHL regulation should apply to cyberspace and cyberoperation, but the boundary for engagement in cyberspace is still unclear and cyberattacks are currently treated as a weapon used in the context of a traditional military engagement, rather than as an independent form of warfare. Most cyberattacks described above occurred outside the context of military conflict between nations and the involvement of government is either being denied or untraceable. Still, the ICRC insist that cyber operations can cause human harm and must therefore by held accountable under the norms of IHL. Their work on the matter concluded in a similar manner, agreeing that IHL "should" apply but wondering how IHL "could" be applied, stressing amongst other things three key problems in the application. Civilian and military targets are not isolated in cyberspace, often overlapping there is no clear distinction made between the two and often military systems use civilian communication channels to operate. This is echoed by this project, even more so when considering that civilian systems have been prioritized over the military targets that protected them, sparing the offensive party a military confrontation to reach the actual pressure point of the attacked nation: civilian infrastructure. What consist an attack is not universally accepted, while the ICRC has issued protocols to this end defining attacks as 'acts of violence against the adversary, whether in offence or in defense' (Gisel & Rodenhäuser, 2019). Echoing the disagreements brought forth by the GGE and the OEWG, disagreement as to how to organize and treat cyberspace as a field of human interactions still impair progress in ensuring peace in cyberspace.

Government and critical infrastructure

The digitalization of every aspects of society is pushing governments to a different kind of governance. Many of the classical aspects of the duties of government, as eclectic might they be from one government to the other, are changing in cyberspace. While theoretically similar in their approach to cyberattacks, state-sponsored hacking and independent hacking from a third party group are still distinct from one another. The funds and capacities of state sponsored hacker groups still have greater impact in cyberspace. While technological progress might change this observation, it is safe to assume for the purpose of this argument that this status quo will remain

for some time. This raise a question in relation to infrastructures, as France has labelled it, infrastructure operators whether private or public are to ensure their own operative security in the physical realm as well as in cyberspace. A similar statement was issues by President Biden following the 2021 colonial pipeline hack, private companies have their own decisions to make. So how are companies, specifically critical infrastructure operators, expected to ensure their own cybersecurity when faced with state-sponsored cyberattacks?

The role of government in critical infrastructure operation is being tested in most western democracies, placing the respect of private property at odds with the security of citizens. There seem to be no straight forward solution to this conundrum, critical infrastructures have been proven to be vulnerable entities and prime target for cyberattacks, and both private and public sectors have faced consequential cyberattacks. This tension relates to the heart of modern democratic governance, where a solution must include a sense of security and an accountable constitutional governance. The reality of the threat posed by advanced cyberattacks on infrastructure requires the full attention of a collaborative effort between the government and the private sector (Shore, 2015). The EU's Cybersecurity Strategy for the Digital Decade includes in its first paragraph the notion that EU citizens deserve a secured and consistent usage of infrastructures and that “The EU’s economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity” (EU commission, 2020).

Arguments have been made in favor of holding governments accountable for upholding critical infrastructure security, binding operation infrastructure with the obligation of state to ensure its citizen’s security (Shore, 2015). Relying on a public/private cooperation seems to be the way currently adopted by most western countries, but the fact remains that governments often fall short of securing cyberspace and are often left to adapt to the evolution of cybersecurity threats rather than keeping up with them.

Conclusion

Cyberattacks and cyberwarfare are an increasingly defining part of modern sociopolitical interactions, this is a reality that we do not yet grasp and have failed to adapt to thus far. Instances of cyberattacks have impacted and impaired critical systems in just about every major aspects of society. While the demonstrated impacts are considerable, the question remains: to what extent does it constitute a credible global catastrophic risk scenario?

Vulnerabilities in governmental systems relating to communications, have allowed hacker to impact mediatic institutions, governmental websites, and governmental agencies. Critical aspects of governmental administration relating to digital ID systems, securing data of national importance, paying pension, and communications with other governments have been shown to be vulnerable to cyberattacks as well. The expansion of E-governance in countries around the world and the established digitalized norm in most western democracies show a clear path of dependence on digital technologies for governmental and administrative institutions. There has also been attempts to disrupt democratic processes at different levels, democratic disruption is a possibility whose extents and veracity is still disputed, and the confirmed instances seem the point towards an increased number of cyberattacks on democratic processes in the future.

The adoption of cyberspace as a field of operation on par with land, sea, and air by every major military power speaks to the significance of cyberspace as a domain of interaction. The nature of cyberspace has hindered effective defense of civilian targets and significantly reduced the role of deterrence in international relations. A new military norm is forming around cyberspace, the safeguards granted by anonymity and the difficulties in attribution favor countries that disregard sovereignty, human rights, international humanitarian laws, and have no system of internal accountability in carrying out attacks. Russia seems to be taking full advantage of this new context, extensively testing its offensive cyber capabilities on neighboring countries as a well as overseas, and slowly forging an indisputable stance as a credible cyber-abled nation. The pursuit of offensive cyber capabilities by military nations risks pushing nations into a context of instability ripe for escalation. The difficulties in implementing existing IHL regulations to cyberspace might indicate the need for a new approach that would appropriately account for the systemic differences between physical and cyberspace. A humbling fact to remember is that existing IHL was slowly built up

from 1864-onwards, with each major conflict being the push bringing together nations to supplement existing norms (1929 Geneva convention, 1949 convention, 1974 Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts) (Alexandr, 2015). The hope being that the international community can experience that push to legislate cyberspace without a major conflict.

Offensive Cyber Capabilities are not developed in a vacuum, while the cyber attacks explored in this paper seem isolated there is no reason to believe that the tools used to scratch the surface of critical systems stop being relevant once deployed. The importance of the solarwind hack has been drastically underplayed as "simple espionage" by the media, the cyberattack successfully infiltrated a key national agency that directly relates to nuclear energy and nuclear weapon stockpile information. The fact that nothing was damaged does not mean that nothing could have been damaged. As Greenberg (2020) and Singer (2014) argue, there is no reasonable scenario where the current "espionage-oriented" status quo does not evolve (or escalate) towards a worse-off version of interactions in cyberspace.

The vulnerabilities exposed in nuclear weapon systems are a grave concern and adds uncertainty to a climate of nuclear tension that is arguably catastrophic in of itself. Atop a climate of nuclear rearmament between Russia, China, and the US, cyber vulnerabilities in the nuclear weapon systems increase the chance of false escalation and/or inadvertent launch.

The critical infrastructure systems have been explored in some depth and multiple key vulnerabilities were identified. The evolution of cyber-physical infrastructure and the adoption of Supervisory Control and Data Acquisition systems have contributed to the development of modern infrastructure but by the same token have opened up a new realm of vulnerabilities in cyberspace. As mentioned throughout the project, the digitalization of critical infrastructures has brought a concrete pressure point of civil society within the grasp of cyberattacks. The interdependency of critical infrastructure and their reliance on the electrical grid has heightened this issue. Furthermore, attack vectors on critical infrastructures can be found both online with classical spread mechanisms and offline by integrating malicious code onto third-party hardware. Energy production, distribution of water, fuel, gas, transport, and electricity, distribution of essential goods and services, communication, public transportation, seaport transportation, air traffic control, manufacturing, hospital and healthcare services, even dispatch of emergency services are all

critical systems that society and people heavily depend on, and their disruption beyond a certain level could prove to be disastrous. This project has showcased few examples of how some of these systems have been temporarily disrupted, and while no human life has been lost as a direct consequence of these attacks, the feasibility of these disruptions lays down a multitude of realistic scenarios where human lives could be at risk.

The discussion highlighted the human element that moderate GCR through prevention and mitigation efforts. In the field of existential risk both on a political and academic aspect, there seems to be a lack of prioritization of the issue of cyber warfare. Instead, futuristic scenarios like artificial intelligence are put in the spotlight by academics and authors. While this issue certainly has relevance in the field, cyberattacks represents a more immediate threat to society. The lack of clarity and established definitions prevents concrete steps to be taken towards stabilizing cyberspace and ensuring its peaceful use. This paper, along with many others, has attempted to provide a valid definition of these terms, and through case studies explored the implications of the nature of cyberspace. However thus far, attempts at a universalization of understandings remain slowed by political agendas and the prioritization of individual interest.

Normative steps have been taken in this regard but more often than not, these soft laws, recommendations and policy guidance rely on good will and due diligence, rather than established framework of accountability. Arguably leaving cyberspace an unregulated and unregulatable entity.

This paper has investigated the topic of cyberattacks through the scope global catastrophic risks methodology and environmental scanning, and has attempted to answer the question: “To what extent can cyberattacks constitute a global catastrophic risk?”

- The nature of cyberspace is fundamentally changing traditional power dynamics between nations, this new and evolving context poses a challenge that I would qualify as extreme, in the sense that it alters universally understood norms and interactions that up until now were taken for granted - accountability, symmetrical power relations, narratives of national defense and sovereignty, the impacts of technological dependence, and a sense of security for a citizen’s future prospects.
- Nation states find themselves evolving in this new context with dated understanding of the power relations in a complex system in dire need of clarity. The problem here is that by

bringing dated realist power stance in a realm as complex and depended-upon as cyberspace, we risk escalation. The international community is witnessing the testing of new advanced cyber weapons on population and civilian infrastructures – the parallel with the bombing Guernica made in the discussion seems all too relevant when applied to the Russian cyberattack on Ukraine. Imagining that these weapons are use in the restricted context of the Russo-Ukrainian conflict is deceptive and if left unaddressed 1) constitutes a form of compliance with the treatment of Ukrainian population (or any other impacted nation), 2) deepens the gap between the offensive cyber capabilities of nations, encouraging armament.

- Every aspects of society have to various extents grown dependent on information and communication technologies and cyberspace, as these dependences grow, so do vulnerabilities. Critical infrastructures are at risk and currently operate at a border between development and catastrophe. Aiming towards development, growth, and security, while increasing the dependency of society on vulnerable system is actively putting the security, prosperity, and human potential of nations at risk.
- Cyberattacks must be recognized in the broader context of their technological capabilities, thus far it seems like governments assess cyberattacks on the merit of their impact rather than acknowledging the attack in the context of what it represents to national security.

In conclusion, and putting aside the notion of nuclear warfare, which in of itself is an undisputed existential threat that is only exacerbated by cyber vulnerabilities in the nuclear weapon systems.

As of the writing of this paper, qualifying the commonly understood notion of cyberattack as an existential threat would be considered an exaggeration. None of the cases explored constitute an existential threat in of themselves, at best cyberattacks are prevented, at worst the nation deals with economic and structural reconstruction. But it seems reasonable to conclude that a simultaneous, coordinated, full-scale cyberattack on all vulnerable critical systems of a society could leave it crippled, result in human casualties, and as seen with the Notpetya worm, spread beyond the initial target through communication systems. The event of such a “worst-case scenario” cyberattack could undoubtedly be a considered a global catastrophic risk scenario, and this paper demonstrates that all the pieces of that puzzle exist in practice.

Further Research

The quantitative limitation addressed in the methodological consideration could prove to be a point of focus of further research. Establishing a quantifiable classification of existential risk could be a useful step in achieving the much-needed understanding of what constitutes a cyberattack and how to address it.

This project was written with the intended goal to build understanding and raise awareness about the reality of cyberattacks and cyberwarfare. The joint publication “assuring our common future” (PNND, 2020) was a step towards raising awareness about the UN disarmament agenda. Having written the section about cyberspace I highlighted good parliamentary practices that could secure a peaceful and sustainable usage of cyberspace. This paper has expanded my views on the matter and returning to the drawing board to investigate cyberattacks as global catastrophic risk from a parliamentary perspective could offer good practices that would be implementable by parliamentarians.

Bibliography

Alexander, A. (2015, March 31). A Short History of International Humanitarian Law. OUP Academic. https://academic.oup.com/ejil/article/26/1/109/497489

Art, R.J. (1980). To What Ends Military Power?. International Security. 4:4 3-35.

Avena, E. (2021, March 11). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop. Microsoft Security. https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Banga, G. (2021, February 26). 8 Common Cyber Attack Vectors and How to Avoid Them. Balbix. https://www.balbix.com/insights/attack-vectors-and-breach-methods/

Banks, W. (2017, November 10). State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. Texas Law Review. https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/

Basu, A., Poetranto, I., & Lau, J. (2021, May 19). The UN Struggles to Make Progress on Securing Cyberspace. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491

Bailey, C. E. (2020). Offensive Cyberspace Operations: a Gray Area in Congressional Oversight. Boston University International Law Journal. Vol 38:2.

BBC News. (2021, April 16). US imposes sanctions on Russia over cyber-attacks. https://www.bbc.com/news/technology-56755484

Beidleman, S. W. (2009). Defining and Deterring Cyber War. U.S. Army War College, Carlisle Barracks, PA 17013-5050.

Bossert, T. P. (2020, December 17). Opinion | I Was the Homeland Security Adviser to Trump. We're Being Hacked. The New York Times. https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html?action=click&module=Opinion&pgtype=Homepage

Bostrom, N. (2002). Existential risks: Analyzing human extinction scenarios and related hazards. Journal of Evolution and Technology. Retrieved from: http://www. jetpress.org/volume9/risks.html

Brodie, B. (1958). The Anatomy of Deterrence. RAND Corporation. Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM2218.pdf.

Brooks, R. (2017, October 6). The Seven Deadly Sins of AI Predictions. MIT Technology Review. https://www.technologyreview.com/2017/10/06/241837/the-seven-deadly-sins-of-ai-predictions/

Brumfield, C. (2020, September 22). The Mysterious Case of the Missing 250-Ton Chinese Power Transformer. Vice News. https://www.vice.com/en/article/v7gaqb/the-mysterious-case-of-the-missing-250-ton-chinese-power-transformer

Bulletin of the Atomic Scientists. (2021, April 29). Doomsday Clock Statement. Bulletin of the Atomic Scientists. https://thebulletin.org/doomsday-clock/

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review. 4(10): 13-21. http://doi.org/10.22215/timreview/835

Crowdstrike. (2016, December 22). Fancy Bear Hackers (APT28): Targets & Methods | CrowdStrike. Crowdstrike.Com. https://www.crowdstrike.com/blog/who-is-fancy-bear/

Davis, P. K. (2015). Deterrence, Influence, Cyberattack, and Cyberwar. International Law and Politics Journal. Vol. 47:327. https://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf

Department of Economic and Social Affairs. (2020). UN E-Government Survey 2020. Publicadministration.Un.Org. https://publicadministration.un.org/egovkb/enus/Reports/UN-E-Government-Survey-2020

Department of Justice of the United States of America. (2020, October 19). Six Russian GRU Officers Charged in Connection with Worldwide. Https://Www.Justice.Gov/Opa/Pr/Six-Russian-Gru-Officers-Charged-Connection-Worldwide-Deployment-Destructive-Malware-And.

Desarnaud, G. (2017). Cyber Attacks and Energy Infrastructures: Anticipating Risks. Études de l'Ifri. IFRI. ISBN: 978-2-36567-724-0

Dowd, K. (2021, May 17). How Private Equity Factors In To The Colonial Pipeline Hack. Forbes. https://www.forbes.com/sites/kevindowd/2021/05/17/how-private-equity-factors-in-to-the-colonial-pipeline-hack/?sh=2c10911d5262

Duforest, A. (2021). Should cyber warfare be considered an existential threat? An investigation of the cyber-attack vulnerabilities of governmental, military, and infrastructure systems. Aalborg University - Department of International Affairs.

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

E.A.S.-Entreprise Estonia. (2021, February 25). We have built a digital society and we can show you how. E-Estonia. https://e-estonia.com/

European Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. Eur-Lex.Europa.Eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

Executive Office of the President. (2020, May 4). Securing the United States Bulk-Power System. Federal Register. https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

FedEx. (2019). 2019 Annual Report Challenge. Change. Innovation. Https://Investors.Fedex.Com/. https://investors.fedex.com/financial-information/annual-reports/default.aspx

Geneva Centre for Security Policy (GCSP), Inter-Parliamentary Union (IPU), Parliamentarians for Nuclear Non-proliferation and Disarmament (PNND), Parliamentary Forum on Small Arms and Light Weapons (PFSALW), & World Future Council (WFC). (2020, November 4). Assuring our Common Future - A guide to parliamentary action in support of disarmament for security and sustainable development. Assuring Our Common Future. https://disarmamenthandbook.org/handbook/

Gisel, L., & Rodenhäuser, T. (2019, November 28). Cyber operations and international humanitarian law: five key points. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

Global Catastrophic Risk Policy. (2021, May 10). Home. https://www.gcrpolicy.com/home

Global Challenges Foundation. (2018). Global Catastrophic Risks Report 2018. The Global Challenges Foundation. https://globalchallenges.org/initiatives/analysis-research/reports/

Global Challenges Foundation. (2020, July 15). Global Catastrophic Risks Report 2020. The Global Challenges Foundation. https://globalchallenges.org/initiatives/analysis-research/reports/

Greenberg, A. (2020). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Anchor.

Haworth, J. (2021, February 10). Researcher hacks Apple, Microsoft, and other major tech companies in novel supply chain attack. The Daily Swig | Cybersecurity News and

Views. https://portswigger.net/daily-swig/researcher-hacks-apple-microsoft-and-other-major-tech-companies-in-novel-supply-chain-attack

Heeks, R. (2001, February 18). Understanding e-Governance for Development by Richard Heeks. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540058

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), 49-60. https://www.jstor.org/stable/26463926

International Committee of the Red Cross. (2004). What is International Humanitarian Law? Icrc.Org. https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf

IDSC. (2000). Civil Information Systems: The National ID Number, IDSC, Cairo

International Telecommunications Union (ITU). (2008). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008

Inter-Parliamentary Union. (2021, January 27). The role of parliamentarians to advance disarmament in cyber space: A focus on cyber-warfare and peace. https://www.ipu.org/event/role-parliamentarians-advance-disarmament-in-cyber-space-focus-cyber-warfare-and-peace#event-sub-page-documents/

Irmak, E., & Erkek, I. (2018). An overview of cyber-attack vectors on SCADA systems. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). Published. https://doi.org/10.1109/isdfs.2018.8355379

Jinghua, L. (2019, April 1). What Are China's Cyber Capabilities and Intentions?. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Labialle, J. C. (2020). "Nous devons mieux nous préparer à un conflit majeur" - Sénat. Sénat.Fr. https://www.senat.fr/presse/cp20200624e.html

Légifrance. (2021). Code de la Défense. Legifrance.gouv. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345191/#:~:text=Les%20op%C3%A9rateurs%20publics%20ou%20priv%C3%A9s,%C3%A0%20leurs%20frais%20dans%20les

Lee, R. M., Assante, M. J., Conway T. (18 March 2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case SANS & E-ISAC https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. IEEE Transactions on Power Systems, 32(4), 3317–3318. https://doi.org/10.1109/tpwrs.2016.2631891

Libicki, M. (2009). Cyberdeterrence and Cyberwar. RAND Corporation. Retrieved March 31, 2021. from http://www.jstor.org/stable/10.7249/mg877af.6

Lilly, B. & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 129-155, doi: 10.23919/CyCon49761.2020.9131723.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (1st ed.). Oxford University Press. https://oxford-universitypressscholarship-com.zorac.aub.aau.dk/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-13

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security, 14(1), 1–33. https://doi.org/10.1145/1952982.1952995

Lord, N. (2020, August 7). The Cost of a Malware Infection? For Maersk, $300 Million. Digital Guardian. https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million#:%7E:text=The%20NotPetya%20fallout%20continues%2C%20with,compromise%20by%20the%20NotPetya%20malware.

Manzanares, V. C. (1997). La destrucción de Guernica: Un balance sesenta años después (Espasa hoy) (Spanish Edition) (Spanish Language ed.). Espasa.

Mark Clayton (2010, September 21). Stuxnet Malware Is 'Weapon' Out to Destroy . . . Iran's Bushehr Nuclear Plant? Christian Science Monitor, 21 September 2010.

Mattila, J., & Parkinson, S. (2017). ECISM 2017 11th European Conference on Information Systems Management. Google Books. https://books.google.cz/books?hl=en&lr=&id=0Yk9DwAAQBAJ&oi=fnd&pg=PA188&dq=ict+military&ots=Um5vKH8Urn&sig=Ui3_n90B6YYJPZHwyys0-3LTZgk&redir_esc=y#v=onepage&q=ict%20military&f=false

McLaughlin, R., & Schmitt, M. (2017, September 18). The need for clarity in international cyber law. Policy Forum. https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/

Meyers, A. (2019, March 29). Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. Crowdstrike.Com. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Minárik, T., Jakschis, R., Lindström, L. (2018). International Conference on Cyber Conflic, & NATO Cooperative Cyber Defence Centre of Excellence. 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. IEEE.

Mowery, S. P., US Marine Corp. (2013). Defining Cyber and Focusing the Military's Role in Cyberspace. United States Army War College.

Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1). https://doi.org/10.1093/intqhc/mzaa117

Nash, K. S., Castellanos, S., & Janofsky, A. (2018, June 27). One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs. Wall Street Journal. https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

United States Congress. (2018). National Defense Authorization Act for Fiscal Year 2019, H.R.5515, 115th Congress (2017-2018).

NBC News. (2019, November 23). Russia Perfected Its Cyberwarfare In Ukraine — America Could Pay The Price | Think | NBC News [Video]. YouTube. https://www.youtube.com/watch?v=nW__A5V-EmQ&ab_channel=NBCNews

NBC News. (2019, November 23). Russia Perfected Its Cyberwarfare In Ukraine — America Could Pay The Price | Think | NBC News [Video]. YouTube. https://www.youtube.com/watch?v=nW__A5V-EmQ&ab_channel=NBCNews

NBC News. (2021, May 13). Biden Speaks On Pipeline Cyberattack | NBC News [Video]. YouTube. https://www.youtube.com/watch?v=NRTFfaV2KOw&ab_channel=NBCNewsNBCNews Verified

NewAmerica. (2019, November 6). Sandworm A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers [Video]. YouTube. https://www.youtube.com/watch?v=41lB6mNrsJY&ab_channel=NewAmerica

NTI. (2020, June). Iran's Nuclear Program Timeline and History | NTI. Nuclear Threat Initiative. https://www.nti.org/learn/countries/iran/nuclear/

Parliamentarians for Nuclear Non-proliferation and Disarmament (PNND), World Future Council (WFC), Geneva Centre for Security Policy (GCSP), Parliamentarians for Global Action (PGA), & Inter-Parliamentary Union (IPU). (2021, January 25). Assuring our Common Future - A guide to parliamentary action in support of disarmament for security and sustainable development. Assuring Our Common Future. https://disarmamenthandbook.org/

PBS NewsHour. (2021, February 23). WATCH: Senate committee hears testimony on SolarWinds hack. YouTube. https://www.youtube.com/watch?v=IPozXgMqMag&t=204s&ab_channel=PBSNewsHour

Pomerleau, M. (2019, June 03). DoD cyber ops are changing, and so is oversight. Retrieved February 15, 2021, from https://www.fifthdomain.com/congress/2019/06/03/dod-cyberops-are-changing-and-so-is-oversight/

President's Commission on Critical Infrastructure Protection. (1997, October). Critical Foundation Protecting America's Infrastructure. Https://Www.Hsdl.Org/. https://www.hsdl.org/?abstract&did=487492

Rees, M. (2003). Our Final Hour: A Scientist's Warning: How Terror, Error, and Environmental Disaster Threaten Humankind's Future in This Century—On Earth and Beyond. New York: Basic Books.

Rees, M. (2004). Our Final Century?: Will the Human Race Survive the Twenty-First Century?. Gardners Books. https://www.penguin.com.au/books/our-final-century-9780099436867

Reuters. (2021a, February 24). SolarWinds hack worse than thought, executives tell Senate. YouTube. https://www.youtube.com/watch?v=Xr9EdOsQx-o&ab_channel=Reuters

Reuters. (2021b, March 1). Mumbai power outage could have been cyber sabotage, says minister. https://www.reuters.com/article/us-india-power-china-idUSKCN2AT31Q

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001, December 1). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Journals & Magazine. https://ieeexplore.ieee.org/abstract/document/969131

Rivera, J., Di Gangi, P. (2020) Assessing Cybersecurity Risks When Adopting Internet of Things (IOT) Devices. SAIS 2020 Proceedings. 15. https://aisel.aisnet.org/sais2020/15

Sagan, C. (1983). Nuclear war and climatic catastrophe: Some policy implications. Foreign Affairs, 62(2), 257–292. https://doi.org/10.2307/20041818.

Satter, R. (2021, May 11). Ransom group linked to Colonial Pipeline hack is new but experienced. Reuters. https://www.reuters.com/business/energy/ransom-group-linked-colonial-pipeline-hack-is-new-experienced-2021-05-09/

Schelling, T. C. (1967). Arms and Influence (The Henry L. Stimson Lectures Series). Yale University Press.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. The Yale Law Journal Forum. Published. http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

Shore, J. M. (2015). An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security. International Journal of Intelligence and CounterIntelligence, 28(2), 236–251. https://doi.org/10.1080/08850607.2014.962356

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know (1st ed.). Oxford University Press.

Smith, R. (2020, May 27). U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny. Wall Street Journal. https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710

Stoltenberg, J. & North Atlantic Treaty Organization. (2019, August 29). NATO will defend itself. Nato.Int. https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

Stringer, D., & Lee, H. (2021, March 3). Why Global Power Grids Are Still Vulnerable to Cyber Attacks. Bloomberg.Com. https://www.bloomberg.com/news/articles/2021-03-03/why-global-power-grids-are-still-so-vulnerable-to-cyber-attacks

Talks at Google. (2014, February 10). Cybersecurity and Cyberwar: What Everyone Needs to Know | Peter Warren Singer | Talks at Google [Video]. YouTube. https://www.youtube.com/watch?v=h0SXO5KUZIo&ab_channel=TalksatGoogle

Thompson, G. (2012). The electronic kairos in Cybercultures; Mediations of Community, Culture, Politics. Reference and Research Book News, vol. 28, no. 1, 2013. ProQuest, https://search-proquest-com.zorac.aub.aau.dk/trade-journals/cybercultures-mediations-

Tikk, E. & Kerttunen, M. (2018). Parabasis Cyber-diplomacy in Stalemate. Norwegian Institute of International Affairs.

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. 2016 IEEE Symposium on Security and Privacy (SP). Published. https://doi.org/10.1109/sp.2016.26

U.S. Cyber Command. (2018). Mission and Vision. https://www.cybercom.mil/About/Missionand-Vision/

United Nations. (2021, March 10). Open-ended working group on developments in the field of information and telecommunications in the context of international security. Undocs.Org. https://undocs.org/en/A/AC.290/2021/CRP.2

United States Airforce & Hill, P. Inc. (2015). Cyber Warfare: Protecting Military Systems. CreateSpace Independent Publishing Platform. https://books.google.cz/books/about/Cyber_Warfare.html?id=a7fPjgEACAAJ&source=kp_book_description&redir_esc=y

United States Army War College, & Mowery, S. P. (2013, March). Defining Cyber and Focusing the Military's Role in Cyberspace. United States Army War College. https://www.hsdl.org/?view&did=815941

US Department of Homeland Security Centre for the Protection Of National Infrastructure. (2011, April). Cyber Security Assessments of Industrial Control Systems: Good Practice Guide. URL: https://www.ccncert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf.

Wade, R. H. (2002). Bridging the Digital Divide: New Route to Development or New Form of Dependency? Global Governance: A Review of Multilateralism and International Organizations, 8(4), 443–466. https://doi.org/10.1163/19426720-00804005

Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats. Momentum Press. https://books.google.cz/books?id=ugOsO17iHB8C&source=gbs_navlinks_s

Woodart, M., Sedigh Sarvestani, S., Hurson, A. R. (2015). A Survey of Research on Data Corruption in Cyber–Physical Critical Infrastructure Systems. Missouri University of Science and Technology, Rolla, Missouri, USA. ISSN 0065-2458