Journal Title
XX(X):1–14
©The Author(s) 2023
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Gentlemen, you can't fight in here. Or can you?: How cyberspace operations impact international security

Sam Maesschalck[1]

Abstract

The military now views cyberspace as a new warfare domain, with constant cyber operations potentially causing significant consequences. Internationally, countries are heavily involved in cyberspace, but international law lags behind this evolution, raising questions about its application and retaliation measures. This paper investigates international law in cyberspace and cyber operations in warfare and terrorism, exploring recent calls for increased legislation. The impact of cyberspace non-regulation on international security is examined from both positive and negative perspectives. It argues that solving anonymity and attribution issues requires state collaboration, with an initial step of cooperation against cyber-terrorism. The conclusion emphasises the necessity of cyberspace regulation and legislation for international and national security, offering a starting point for discussion.

Keywords

Cyberspace, Regulation, Cyber War, Cyber Terrorism, Security

Introduction

Over the past few decades, cyberspace has grown increasingly important globally, transforming the Internet into a truly worldwide network. The incredible pace of development in this domain is astounding, as evidenced by the evolution from ARPANET (Lukasik 2010; Abbate 2000) in 1969 to the modern Internet we know today, a process that took roughly 20 years and involved numerous experts and intermediate stages. The evolution from ARPANET to the first stages of the modern Internet, where individual networks that were being linked together, involved many experts and intermediate stages and was managed in about 20 years (Leiner et al. 2009). Presently, our daily lives are filled with internet-connected devices, from coffee machines and fridges to cars with data connections. Having multiple internet-connected devices has become a normality that is becoming more ingrained in our lives and Internet access itself has been deemed a human right by the United Nations (2016). This widespread connectivity is also prevalent among governments and militaries worldwide, who now rely on the Internet for warfare (Harris 2014) and are developing an Internet of Military Things (Banerjee et al. 2018). Not only do we use more devices connected to the Internet, but we are also moving to e-governance, where the Internet becomes the route for citizen engagement and participation with the government (Baxter 2017). While the growth of cyberspace brings numerous advantages, it also presents challenges for both nations and individuals, necessitating efforts to ensure its safety through both technical and non-technical means. In regards to the military, there have been many studies into the rise of the fifth military domain, which encompasses cyberspace. However, this falls outside of the scope of this study. Military and intelligence sectors have rapidly adopted cyber capabilities, raising questions about the benefits and drawbacks of this

[1] Security Lancaster, Lancaster University

Corresponding author:
Sam Maesschalck, Infolab21, Lancaster University,
Lancaster, LA1 4WA, UK.
ORCID: 0000-0003-4609-3487
Email: s.maesschalck@lancaster.ac.uk

development and its implications for international security. This paper argues where some of the benefits and downsides of this adoption lie and their impact on international security.

One of the most appealing aspects of cyberspace is its relative anonymity, where consequences for actions can be escaped from. This leads to the space being used for activities that might be viewed as improper. Aside from surveillance on enemies, cyberspace makes surveillance on allies possible, which is a common action that countries take within it. This anonymity is an important aspect and can also have another use aside from providing anonymity, as can be seen in the development of onion routing by the US military (Goldschlag et al. 1996). However, onion routing is currently very much embraced by people with the so-called Darknet (Mirea et al. 2019; Bancroft and Scott Reid 2017) because of its increased anonymity and is used for illegal activities. There are many issues related to the regulation of cyberspace from an international perspective, which have to be explored and solved before legislation can be adopted.

International security is a dynamic yet enduring concept, affected by the emergence of cyberspace and the new challenges it poses. The rise of cyberspace posed new challenges and aspects of international security we have to take into account and change how it could be impacted. While the nature of threats has evolved, the potential impact on society remains largely constant, as cyber warfare still threatens civilians and critical infrastructure. This can be linked to how warfare has changed, but the potential impact has remained consistent. If we think about cyber warfare, it still impacts civilians. It can still disrupt the same processes such as energy distribution and the governmental/democratic processes as a whole or in part. Generally speaking, the threats evolve, but the potential impact remains the same when looking at international security.

Achieving national security in an increasingly interconnected world necessitates international cooperation. We can all agree that the world has become a more global place, where we are not only affected by our immediate neighbours, but we can now be affected by situations on the opposite side of the planet. National security in this global environment can only be achieved through international cooperation (Dannreuther 2014). We focus on the effects cyberspace can have on international security. However, due to the prevalence of cyberspace, there is much overlap with non-cyberspace aspects or broader aspects that do not just include cyberspace. The field of international security has grown out of the questions of how we can protect a State against threats from both internal and external threats, mainly after World War Two and after taking the globalisation of the world into account (Buzan et al. 2009; Cha 2000).

This paper aims to explore current legislation regarding state actors in cyberspace, as well as cyber warfare and terrorism. The paper will examine the advocates for increased regulation and the impact of cyberspace on international security before discussing potential approaches to addressing key questions related to legislation and regulation. The study will also consider the challenges of applying international law to cyberspace and the reasons for states' reluctance to support regulation. Then there is a brief discussion on the first steps on how the key questions relating to cyberspace legislation and regulation could be answered.

Cyberspace Legislation

Legislation governing cyberspace faces multiple challenges. Foremost, it must gain universal acceptance from all countries, a feat that proves exceedingly difficult to accomplish. Even if consensus were achieved, enforcing such laws poses significant obstacles. The Tallinn Manual 2.0 by Schmitt (2017), the primary literature on international law within cyberspace, offers guidance on the application of international law in cyberspace. However, the Manual is non-binding and not recognised as part of international law. It expands upon its predecessor, the Tallinn Manual on the International Law Applicable to Cyber Warfare, to encompass all operations in cyberspace. The practice of creating non-binding interpretations of laws is not new and has occurred previously in relation to armed conflicts at sea (Doswald-Beck 1995) and air warfare (Bruderlein 2009).

The Tallinn Manual 2.0 outlines black letter rules, which are actual laws within international law, but have yet to be applied within the context of cyberspace. This highlights a challenge in regulating cyberspace, as even established international law can be difficult to enforce (Fitzmaurice 1956). The anonymity that cyberspace affords further compounds this issue, making it challenging to attribute responsibility to actors that violate international law. A closer look at the Tallinn Manual 2.0 reveals interesting discussions regarding cyberspace.

The Manual's first rule pertains to the principle of State sovereignty, which is crucial to establish in any domain. Without sovereignty, it is difficult to claim one has been attacked. Thus, if a State does not have sovereignty in cyberspace, it lacks jurisdiction or independence within it. While the Manual acknowledges that the principle of sovereignty applies, there is no consensus about this (Mueller 2020). Establishing clear sovereignty in this space would be a remarkable achievement and would create a broader foundation for regulating cyberspace. However, achieving consensus among the international community remains challenging. To assert power in cyberspace, a State must establish jurisdiction within it. However, this, too, hangs in the balance since jurisdiction is closely linked to sovereignty. The Tallinn Manual Experts are clear in their view that a State has jurisdiction over cyber activities (Rule 8). Nevertheless, a lack of consensus on sovereignty means that there is no clear agreement on this (Assaf and Moshnikov 2020).

In 1996, the famous 'Law and Borders: The Rise of Law in Cyberspace' was written by Johnson and Post (1996), which debated how cyberspace was an entirely separate space where territorial jurisdiction and borders made no sense as it was not a physical space. Given that cyberspace has a physical aspect, such statements are exaggerated. Over the two decades since the publication, our notion and the importance of cyberspace have changed tremendously, leading to many efforts to investigate legislation within cyberspace.

Defining wrongful acts within cyberspace is vital. Rule 14 of the Tallinn Manual 2.0 states that an action within cyberspace that constitutes a breach of an international legal obligation is a wrongful act. It explicitly references that the breach must be attributable to a State. However, as mentioned earlier, if there is no precise legislation defining wrongful action, or if it is not feasible to attribute an action to a State, how can this be acted upon? Legal operations can constitute a 'use of force,' which is an unlawful act inconsistent with the purpose of the UN or that affects the territorial or political independence of a State. In cyberspace, not all actions constitute a use of force, such as cyber espionage (Schmitt 2010). Other operations can have a high impact, such as the destruction of infrastructure, which is possible via a cyber attack. Especially as technology within our most critical infrastructure, now connected to the Internet, has major vulnerabilities that could lead to disastrous effects (Maesschalck et al. 2023; Andrew et al. 2020). Rule 68 within the Manual discusses this and expands upon this in Rule 69, where they agree that a cyber operation with effects comparable to an operation that constitutes a use of force in a non-cyber operation does constitute a use of force. We would agree with that. However, to fall under the use of force, we have to link this back to territorial and political independence, which is difficult to assess as there is no consensus on sovereignty. Further, due to the nature of cyber operations, their effects can be difficult to compare to the effect of traditional (physical) operations. For a country that heavily relies on cyber infrastructure, a disruption might also have a more significant impact than a less reliant country.

Aside from the current international laws we have, there is no binding international consensus on what is allowed and not within cyberspace. As discussed, the Tallinn Manual aims to provide an interpretation, but to this moment, it does not represent the view of States or even NATO CCDCOE who requested it. This leads us to question why it was requested and, more importantly, why states and international organisations like NATO do not want to support the Manual or specific laws regarding cyberspace operations actively.

Warfare in Cyberspace

With the internet evolving from a US Military project, we must question how it can be used in a military matter. The concept of cyber warfare or cyber war can seem daunting, but given the track record humanity has with exploiting technologies for warfare purposes, it can be a real possibility. Some experts within the field have argued that cyber war would never take place; the most prominent of these is Rid (2012). Other experts like Arquilla and Ronfeldt (1993) have clearly stated that cyber war is coming, and Clarke and Knake (2014) have said cyber wars or smaller versions of it are already happening. It is indeed true that cyber operations bordering warfare have already happened. Prime examples of this are Stuxnet (Farwell and Rohozinski 2011) and the cyberattack on Estonia in 2007 (Schmidt 2013). With Stuxnet even being used in the discussion on the future of cyber war.

Although it seems like Rid's claims on cyber war are dismissed here, he does make a compelling case. These claims on how cyber is not a new form of war itself but rather a new form of carrying out activities that were already carried out are valid. However, due to the significant expansion of the internet and cyberspace as a whole, it becomes a more likely target rather than a tool within traditional warfare. Additionally, it means that a cyber attack can potentially have a more significant impact than ever before. This can also be seen from both the United States Cyber Command and the United Kingdom National Cyber Force initiatives.

Our main argument in support of cyber warfare is that it presents a low-cost but high-impact method of conducting military operations, which could be advantageous for countries that lack traditional military power. Moreover, the anonymity of cyber operations creates opportunities for states to engage in attacks against other nations without being overtly involved in war or even targeting their allies. States can also use third-party organisations to conduct cyber operations on their behalf, thereby minimising the risk of exposure. This approach is similar to the use of paramilitary groups by states to conduct covert operations outside of cyberspace. However, several factors pose risks to exposure, such as the capture of operatives and money trails. With the advent of cryptocurrency, the money trail can be obscured, making it more challenging to trace. The Tallinn Manual Rules 90 and 91 address the treatment of mercenaries or civilians participating in state cyber operations, indicating that this is a common practice in cyberspace. For instance, during the Estonian cyber attacks, forums in the Russian language described ways to harm Estonian servers, demonstrating the use of non-state actors in cyber operations (Schmidt 2013). This is also discussed by Maurer (2018), who points out that China relied on militias at the end of the 20th century to conduct cyber operations. Another example is the cyber attack on the Ukrainian energy systems in 2015, which caused widespread consequences. Although there is no clear evidence, Ukrainian intelligence believes that the Russian state was involved (Shehod 2016). This incident illustrates the impact a purely cyber operation can have on the physical world and its potential for military application.

An emerging trend in international relations is the increasing reliance of nations on cyberspace to conduct operations. Recent revelations indicate that the US National Security Agency has been involved in the cyber espionage of EU senior officials through a partnership with the Danish foreign intelligence unit (Reuters 2021). It is not the first instance of cyber operations conducted on nations by their allies, as there is evidence that similar incidents have taken place within the NATO alliance (Easley 2014). While such actions do not amount to full-blown warfare, they could be employed to gather intelligence during an armed conflict or to strain relationships between states.

Terrorism in Cyberspace

Cyberspace constitutes a public domain that extends beyond the purview of states. A vast majority of individuals access the Internet, a component of cyberspace, for work or leisure. This includes malicious actors, such as hackers and fraudsters, and state-sponsored cyber-terrorism activities. A recent instance of cyber-terrorism involves the Islamic State's Cyber Caliphate (Liang 2017). The increasing prevalence of cyber-terrorism can be attributed to the anonymity and ease of engagement within cyberspace, which is also helped by the non-cooperation of states within cyberspace. This also applies to individual actions and hacker group activities, such as the well-known Anonymous (Olson 2013), which has orchestrated numerous cyber-attacks against governments and corporations. Hacktivism has emerged as a significant term within both scholarly research and daily discourse, particularly as younger generations become more technologically proficient. This phenomenon is expected to expand further. The appeal of conducting cyber-attacks lies in the ability to disrupt entire organisations rather than protesting in front of a building.

While anonymity remains relevant in hacktivism and cyber-terrorism, legislation targeting non-state actors exists. Examples include the U.K. Computer Misuse Act, the U.S. Computer Fraud and Abuse Act, and the EU Directive on attacks against information systems (2013/40/EU), which provide a foundation for member-state legislation. Consequently, non-state actors engaging in illicit activities within cyberspace can face legal repercussions. However, enforcing these laws remains challenging. If an actor is apprehended, jurisdictional issues may arise, particularly if the perpetrator or crucial investigation data is located in another country. Such jurisdictional complications can significantly hinder cyberspace investigations (Ghappour 2017).

Numerous recent attacks exemplify terrorism, hacktivism, or non-state actor involvement. In February 2021 (Vera et al. 2021), an unidentified hacker infiltrated a Florida water treatment plant, attempting to alter a chemical compound level in the treated water drastically. The perpetrator's identity and location remain unknown. This highlights the vulnerability of critical infrastructure connected to the Internet. Another water treatment plant attack occurred in January 2021 in the San Francisco Bay Area (Collier 2021). The attacker exploited a former employee's TeamViewer credentials, allowing remote access to the facility and the subsequent deletion of several programs. No incidents were reported, demonstrating that extensive hacking knowledge is not always necessary to compromise critical infrastructure. cyber security is a collective responsibility, as a single weak point can have significant consequences.

The United States recognises the importance of cyber security, with President Biden signing an executive order to enhance national cyber security (The White House 2021). The order emphasises collaboration between the Federal Government and the private sector, which is crucial for bolstering security. The interdependence of private and governmental systems can be exemplified by the NotPetya attack on Ukraine, which also affected private entities such as Maersk (Ritchie 2019).

The year 2014 was notable for cyber-terrorism. Brill (2015) documented cyber-terrorism incidents throughout that year, including the Sony Pictures data breach and the release of ”The Interview,” which was accompanied by terrorist threats. Several theatres initially opted not to screen the film, but Sony later reversed the decision. This episode illustrates the increasing ease with which non-state actors can influence events within other nations. The primary motive for cyber-terrorism and cybercrime is financial gain, followed by commercial espionage and hacktivism. These motives are analogous to other criminal activities; however, cyberspace further connects criminals and terrorists. Cyber-terrorism acts need not be confined to conventional criminal or terrorist activities. In 2021, an unidentified party potentially instigated a cyber operation that could have escalated to warfare between NATO and the Russian Federation (Sutton 2021). The operation interfered with the tracking data of two NATO warships, specifically the AIS signal. While the ships were actually positioned near Odesa in Ukraine, the manipulated data indicated they were close to the Russian-controlled naval base in Sevastopol, Crimea, approximately 300 kilometres away. If NATO had indeed placed two warships near the naval base, it would have constituted a highly provocative action, given Crimea’s disputed status. Russia might have perceived this as a threat to their sovereignty and possibly taken action, even though the international community does not recognise Russia’s annexation of Crimea. The increasing dependence on technology within defence systems underscores the potential for severe consequences resulting from data disruption or falsification.

Advocating for Regulation

The call for regulation and legislation within cyberspace is not new, and the challenges of regulating this domain are multifaceted. While the Tallinn Manual has provided an international law perspective for cyberspace regulation, the issue of civilian usage of cyberspace remains contentious. Discussions have emerged regarding the self-regulation of the Internet (Price et al. 2005) and the right to privacy (Bowie and Jamal 2006). Nevertheless, here again, the anonymity and nature of cyber come into play. How can we regulate something we cannot necessarily see or know the full extent of? The exact size of the Internet is almost impossible to measure. The Surface Web, which most people view as the Internet, is only a tiny fraction of the whole Internet itself. There is the Dark Web, which is in most views linked to criminal activity, is inaccessible via the search engines we most use and hosts sites built especially with anonymity and encryption in mind. The Dark Web is a small fraction of the Deep Web, which encompasses all sites that are somehow protected from public access. This includes websites we all very regularly use, such as our email account and other sites that have to be accessed through another site or require an account to access. Therefore, the issue of regulation lies with the anonymity of the user and the fact that no one knows the full scale of the Internet.

Despite these regulatory challenges, organisations continue to call for and work towards regulation. It also does not mean there is no need for regulation. Europol, for example, has been one of the international organisations that put pressure on cybercrime legislation in its 2016 Internet Organised Crime Threat Assessment (IOCTA). So far, 79 states have shown their support, alongside hundreds of organisations and companies, for the Paris Call For Trust and Security in Cyberspace. Fundamental principles of the call include protecting individuals and infrastructure, preventing activity that damages the availability or integrity of the public Internet, defending electoral processes, and promoting international norms of behaviour. This shows promise, but important States such as Russia, China and the USA did not participate in this call. However, it does not mean there are no efforts from a truly global organisation. In 2016 the United Nations (UN) held a conference on Cyberspace and International Peace and Security, during which the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security presented their work. There is also a second group within the UN, established under GA resolution 73/226, called Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security. Aside from these groups of experts, there is also a UN Open-Ended Working Group on Developments in the Field of ICT in the Context of International Security. This shows that cyberspace is a fundamental topic the UN is working on. One major feat of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security was establishing that international law applies to cyberspace, on which the latest report of the GGE on Advancing responsible State behaviour in cyberspace in the context of international security (United Nations 2021) builds upon. This report was the final report of this group and has been presented to the 2021 General Assembly. This is an essential first step on the roadmap to achieve regulation within cyberspace, but acknowledging that international law is applicable does not mean the issues described earlier are answered. For example, there is still no internationally agreed definition of cyberspace as there is merely a reference to the interdependent network of information technology.

From the Paris Call, we can identify that several world powers did not sign up for it. Does this mean something? Especially when progress is being made by the United Nations, which should have the support of all nations. This is a difficult question to answer. These two initiatives aim to establish some form of legislation or international law for cyberspace but are also key differences. The Paris Call incorporates some specific key aspects all countries that sign up to it support. Be it the defence of electoral processes or the call to exchange information on ICT-related incidents between States. Signing up to this would mean a State promises to uphold these principles, and non-corporation with other States would potentially anger the other nations that have signed up to the principles. In a way, the countries' governments signed up to the call would have to appear to at least follow them. This would mean sharing some information and taking visible actions in relation to the principles.

The UN charter is less specific, and particularly within cyberspace, there are still many questions about how these would actually map to cyber operations. This grey zone gives States some wiggle room and would present only minor implications. Until there is a precise mapping of current international laws to cyberspace or a new set of international laws for cyberspace, the acceptance that international law is applicable to cyberspace does not lead to a significant change. Looking at the Tallinn Manual, we can see that the experts who came together to define how these laws are applicable did not always find a consensus. Can we expect all nations within the UN to agree? The problems of sovereignty, non-intervention and others are extremely challenging to solve. If certain States are happy with the current state of ambiguity, why should they make any real effort to fix it? Maybe it takes a real cyber war for countries to come together as they would see what the effects of such a war would be. Maybe we first have to solve the problem of anonymity from a technical perspective, so there is no real benefit to the non-regulation anymore? We can ask many questions, or there are many assumptions we can make regarding why States would oppose cyberspace regulation. Nevertheless, if they are satisfied with the current status quo, there is no reason to help change it.

Lastly, we also have to remember the efforts made by NATO to legislate and regulate the area of cyberspace. Not only by inviting experts to write the Tallinn Manual but also by accrediting the Cooperative Cyber Defence Centre of Excellence back in 2008, NATO showed how important cyber was and will become. The centre also recognises the multidisciplinary aspect of cyberspace and how issues like legal aspects of cyber defence have to be looked at alongside standards, practices and military doctrine. If the UN cannot agree with a unitary voice on the issues related to cyberspace, maybe we need to rely on these other international co-operations with countries that are more willing to take the initial step towards legislation and regulation. Through this, similar to the collective security aspect of NATO, we might achieve more serious repercussions for nation-state cyber operations. This could then provide deterrence and possibly be the first stone in achieving UN-wide cooperation on the issue. The path towards effective regulation of cyberspace remains fraught with obstacles, and the involvement of various stakeholders, including states, international organisations, and non-state actors, is critical for success.

International Security and Cyberspace

One recurring theme throughout this paper is the anonymity inherent in cyberspace. Again, that particular characteristic is vital in international security and how it allows cyberspace to have such a significant effect on it. This is also further strengthened by the UN OEWG on developments in the field of information and telecommunications in the context of international security (UN General Assembly 2021) report, which notes the increased reliance on ICT throughout the pandemic, how development within these areas have implications across all pillars of the UN (including peace and security) and how maintaining and building peace, security, cooperation and trust within this environment is paramount. They further note how negative developments, such as the use of cyber for malicious purposes, can impact human rights and fundamental freedom.

Instances of state-sponsored cyber espionage are pervasive, with recent revelations involving third-party intermediaries. As discussed previously, back in May 2021, America was caught spying on Germany's Chancellor, Angela Merkel, and other top European officials with the cooperation of Denmark (Reuters 2021). Another significant espionage attack conducted through cyberspace which involved 30 000 organisations, has recently been brought to light (NCSC 2021; Burt 2021). Allegedly perpetrated by a Chinese-sponsored group targeting Microsoft Exchange servers used by numerous organisations worldwide. This attack represents one of the most extensive cyber espionage operations against the UK and its allies to date. Cyber espionage attacks would be one of the more straightforward and concealed operations to conduct within cyberspace as it should not involve any interaction with the systems aside from accessing them; if it does, it would not be purely cyber espionage.

A pertinent question concerning such cyber operations is whether they truly pose a threat to security or merely reflect the complex trust dynamics between nations. One might expect cooperation and collaboration between countries within defensive alliances, such as NATO, or political and economic unions like the European Union. However, in this one example of cyber espionage, we can see a NATO country spying on other NATO countries that are part of the EU through a nation that is part of the EU. This might show that there is still a level of distrust between these States, or it could show a general level of caution. Going back to the relatively low impact of an attack like this, as there are no damages nor direct interference with any sovereign matters aside from espionage, is this a flawed approach? Does cyber espionage improve international security? If every country spied on each other, there might be a stronger case to trust and collaborate. Non-regulation allows nations to be freer in their operations within this space; if intelligence agencies find a potential risk towards their country, appropriate measures might be put in place. To achieve a level of effective collaboration we must take into account the design and formalisation of negotiations and institutions (Lenz 2018) needed to develop clear regulations of cyberspace. In the current state of cyberspace, rapid actions are feasible due to the absence of clear legal frameworks that might impose time constraints or limit potential actions.

However, counterarguments also hold merit. If nations trust each other solely based on their perceived trustworthiness, can genuine trust be established? Would knowing one is under surveillance prompt even greater secrecy and operations within entirely isolated environments? If cyberspace is employed to bypass other international laws and fundamental rights, such as international human rights, could be jeopardised. Cyberspace regulations could affect the actions States could do within cyberspace and have an effect on civil use of the environment. It is impossible to clearly define when an actor is working from their own initiative or when a State sponsors them. This could lead to nations imposing more restrictive Internet access to protect themselves from potentially breaking international laws. Negative consequences of not regulating cyberspace extend beyond the realm of international relations. For example, suppose cyber espionage is the norm. In that case, countries will be less encouraged to report vulnerabilities found in software or even expect businesses headquartered within their country to implement backdoors. This can be seen in the well-known case where the FBI had issues to crack an iPhone that was involved in a shooting at a US Navy base (Leswing 2020). In this case, the US Attorney General and President Trump wanted Apple to help to unlock the phone and, to a further extent, implement a backdoor as they believe law enforcement should have access when needed. Another example can be found within the UK, where the government is pushing to stop end-to-end encryption of messaging apps as encryption makes it harder for investigators and technology companies to monitor activity (Volpicelli 2021). As many governments use similar software (e.g. Microsoft Windows), there is at least one reason they would be inclined to encourage developers to patch their software. However, we do see this is not the case as a lot of actively exploited Windows vulnerabilities still do not get patched immediately even when they become public knowledge but only after they lost control of it Wicker (2020). This shows both the benefits and downsides of encryption, which are shared by other security technologies, as we cannot choose only to encrypt non-illegal messages. However, lowering encryption does not only help law enforcement but an actor, such as other nation-states, that might want to read into conversations. From a pure security perspective, any vulnerabilities should be reported instead of being used by the private or public sectors to gain access to a system. These vulnerabilities do not just allow one nation to access a system but everyone who finds it, including actors with more intrusive goals.

Examining non-state actors, terrorists would undoubtedly benefit from discovering vulnerabilities and maintaining the status-quo related to anonymity. Given that States might not report these so they can exploit them or have businesses implement backdoors for them. These vulnerabilities and backdoors can be found and exploited by anyone else, including terrorists. Additionally, many of these vulnerabilities can be used for more than just espionage but also for disruptive operations. These could have significant consequences when found by certain people and could be seen as an indirect risk related to the normalisation of cyber espionage. Therefore, an argument can be made that although the act of cyber espionage in itself does not have a significant impact, the environment that enables these operations can allow more impactful operations to occur. By making this association, cyber espionage can significantly impact international security. Linking this to the movement to connect critical national infrastructure to the Internet such as stated by Miller et al. (2021), there are clearly significant threats related to this. Within the paper, there is an overview of many attacks that involve critical infrastructure, the impact they had, and how they have evolved over the years. Although there is a lot of regulation within this space related to the security of these systems (Maesschalck et al. 2022), these have not stopped nation-states or non-state actors from infiltrating the systems. Dealing with nation-state threat actors requires a different approach than other threat actors (Derbyshire et al. 2018, 2021) and the cooperation of states on this is crucial as they can work towards the identification of these actors by collaborating on investigations. Undoubtedly, espionage can have serious consequences related to leaking confidential information such as intellectual property or prototypes.

However, its direct impact on the systems involved in the attack is minimal, unlike the Black Energy attacks on Ukrainian energy systems (Khan et al. 2016). Therefore, the impact of espionage is dependent on the information gathered and does not always have to have an impact. The impact also differs when considering which nation is spying on which nation. Allies spying on allies will have a lower impact than enemies spying upon each other. In comparison, a disruptive cyber operation on systems generally has an immediate impact that can be significant and involve civilians. Cyber operations can also be used to affect vital processes in our society but have no physical impact. One example of this is how elections can either be influenced by fake news and propaganda from another nation-state or directly by hacking the electronic/Internet voting systems. Evidence has been found during the 2016 US elections that Russia targeted elections systems within all 50 US states and that Russia used all major social media platforms to meddle with the election (Senger and Edmondson 2019; BBC 2018; US Senate 2019). These actions clearly interfere with internal State affairs but nevertheless go unsanctioned. Other actions such as blocking communications, falsifying information, or even launching an attack in such a way it looks like it comes from another nation can significantly impact a State or the international community. Many of these attacks are solely possible because of both the increased connection of systems and processes to the Internet and the lack of security incorporated within them. Although, even the most secure system can have vulnerabilities, and the adoption of the Internet or technology as a whole into specific processes inherently opens them up to threats and lowers the trust we can place in them. Going back to elections, electronic voting has many potential risks inherent to the technology. The devices' operating system can be corrupt, and the votes can be corrupted when taken off the system. Devices like USB sticks might be used to tamper with the votes, and many other scenarios are possible. More practical examples of vulnerabilities within voting machines are reported by Blaze et al. (2017) from an event at DEFCON 2017 where they had 25 systems used within elections in a hacking village which they opened up for participants to hack.

It is clear that many nuances can be made with cyber operations, as there is a broad range of operations possible within cyberspace. Thinking back to cyber espionage operations, there are some benefits to international security because of them. Nevertheless, there are also many indirectly related threats, such as obtaining information without the appropriate setting. Looking back at the impactful study by Johnson and Post (1996), this new world screams for clear laws and regulation, just as what happened when humanity took to the skies, space, and developed nuclear weapons. New advances in warfare and international politics must be followed by advancements in law. Given all the activity that is going on within cyberspace, both by States and other actors, many risks are taken daily.

On the one hand, we have this environment where we rely more on it daily. On the other hand, we fail to establish clear boundaries and appropriate conduct within them. Why do we manage to create laws that govern private citizens within cyberspace but fail to do this for nations? Why not hold them to the same standard? If it is clear a private citizen cannot tamper with a system that does not belong to them, why is a State seemingly allowed to do so? This state of non-regulation does also assist terrorists and disruptive actions by nations without a legal route to retaliate, aside from some actions like publicly calling another nation out for their attack or putting limited retaliations in place such as embargoes. The international community does recognise the threats faced due to the adoption of cyberspace but is also cautious about adopting any steps towards regulation that would clearly improve international security. One of the reasons can be the anonymity of cyberspace, which is evident. Any actions taken against cyber operations have to be appropriate, and many reports include 'alleged' or other notions that there is uncertainty about the actor that conducted the attack. So we have to ask the question if regulation in an anonymous environment is actually useful or feasible? This question has to be solved and leads to the question of whether non-regulation contributes to anonymity. If there are no laws, solving anonymity itself does not lead to anything. The issue of anonymity can potentially be solved when there is collaboration between the international community and technical experts. Related to the applicability of international law, it is clear that it is applicable, and activities such as the Tallinn Manual can help us establish how current laws fit within this environment.

Further to this, essential aspects such as sovereignty and jurisdiction have to be solved from a legal perspective. If the community pushed towards regulation, there would be a need for new laws that incorporate all aspects of cyberspace. Currently, law enforcement has issues conducting investigations within cyberspace due to lack of access. If laws required cooperation by both States and organisations alike, these investigations would be easier. However, if the international community's goal is to avoid surveillance and attribution at all costs, they have to accept all the risks that come with it.

A prime example of this is the Darknet which uses TOR (The Onion Router), which was initially a military project by the US Naval Research Laboratory to avoid detection (McCormick 2013). Nowadays, TOR is generally known for its more malicious purposes as it provides them with a highly anonymous environment. However, it is important to note that it is also used for non-criminal purposes, as evidenced by Mirea et al. (2019). This evolution does show that research that might have been conducted with the best intents of keeping operatives safe can also be used for the wrong purposes when other people get access to it.

Towards Regulation in Cyberspace

Suppose we want to achieve progress toward cyberspace regulation, the questions identified in this paper have to be answered. One of the main hurdles to figure out is cyberspace sovereignty, which is fundamental to establishing law in this space. The other crucial question to answer is how attribution can happen within this anonymous environment. Both these questions present many hurdles and cannot be answered quickly. If this were the case, we would already have answered them. These challenges and the fact cyberspace is one of the last remaining non-regulated field that has been a holding back the calls for regulation and the initiatives from the UN.

As established before, sovereignty is often linked to the physical domain, such as land borders that have been established. Within cyberspace, this might seem to be impossible to apply in the first instance, as we mainly view cyber as a virtual domain. However, there is very much a physical aspect to the space. Actions and data in cyberspace are not purely virtual as they lead to actual changes on things such as hard drives and how systems operate. Often, our actions do not significantly impact the physical world, but systems such as industrial control systems do. These systems control many devices that we interact with in our daily lives, such as HVAC systems and traffic lights, and operations that play an important role in society, such as energy production. Therefore, the argument can be made that interacting with one of these systems located within a sovereign county can be a breach of the sovereignty of that country. The lack of people crossing the border is not an argument against this, as unmanned drones crossing borders is a breach of sovereignty as well. A caveat we have to make is related to the use of cloud services, which can be located in another country. In this case, we have to determine the ownership and sovereignty of the data located on those systems. This could potentially be viewed in the same way as to how laws (e.g. GDPR) still apply to nationals abroad, or an arrangement can be made similar to how embassies operate. Additionally, data itself can fall under the same concept of sovereignty as the data itself is owned by the country, and any deliberate breach of CIA (Confidentiality, Integrity and Availability) by another country constitutes a violation of sovereignty. Overall, this requires the start of 'cyber diplomacy', where countries can engage by establishing bilateral and multilateral dialogues to discuss cyber threats, share best practices, and collaborate on investigations related to cyberattacks. For this we should build upon initiatives such as the NATO CCDCOE from a non-military/defence focus keeping in mind the requirements for effective intergovernmental cooperation as the feasibility of a solution might change because of it. In addition to the development and implementation of strong legal frameworks to prosecute cybercriminals, including nation-state actors, and provide assistance to other countries in their efforts to do the same.

The more difficult question is related to the anonymous aspect of cyberspace, as this is an inherent characteristic of the space. We need to address this before any advance can be made towards applicable legislation and regulation. Although we can base an actor's location by locating the IP address linked to them, technologies like VPN can easily be used to obfuscate this and is also an important technology for legitimate users to keep their data safe. In international disputes, attribution is based on likelihood and assumptions, which are themselves based on a subjective opinion, such as how certain state groups generally write code. These can be easily used to make a system (e.g. a virus) portray like it was developed and deployed by a particular state actor and potentially deteriorate relations between States. Therefore, anonymity is difficult to work out. Nevertheless, when there is more state cooperation and the potential for actual repercussions after a cyber attack, the path the attack has taken might be able to be uncovered. More precise attributions can be made by following the attack throughout cyberspace and how it traversed through cyberspace. State cooperation to investigate cyber operation is one of the few ways anonymity within the space might be broken, particularly as not all countries have the resources or experience to investigate cyberspace. Establishing a consortium of countries that actively work together to attribute cyber operations to actors, within and between the current alliances, will be the first step towards making cyberspace less beneficial for aggression between nations. This can also lead to the provision of cyber capabilities between countries within the consortium, as is currently done within warfare situations as well.

However, one key element of this debate, which is often referred to, is the major technology firms where data is stored and passes through. These organisations often hold crucial data to unveil who is behind cyber operations, which many countries have their eyes upon. This is understandable, but poses a significant risk to international security as well. When governments advocate for the abolishing of vital security measures such as encryption, this also poses serious risks to citizen's privacy and security which does not outweigh the risks. Forming partnerships between governments, private organisations, and cyber security firms can help pool resources, knowledge, and expertise. This collaboration can enhance the ability to detect and attribute cyberattacks to nation-states as long as these are not directed at a blanket ban or backdoor into systems which will reduce security for all. These partnerships should also include a focus on specific industries and their unique cyber threats, which can help identify patterns and behaviours that may be attributed to nation-state actors targeting those industries. This all should feed into a bigger picture of investing in the development and training of cyber security professionals will improve the capacity to detect, analyse, and attribute cyberattacks. This includes sharing best practices, providing training, and establishing centres of excellence to foster expertise in cyber attribution from public and private sectors based on international collaboration. Within these centres of excellence and partnerships, a focus should also be on the sharing threat intelligence related to cyberattacks can help improve attribution capabilities, which is often a significant hurdle.

A potential concrete first step that can prove to be beneficial in working towards the goals discussed is to find a common factor where all nations would benefit from cooperation. For this, we can look at institutions such as Interpol, which already works together across 195 member states to tackle crime. In a similar line the establishment of an international organisation to tackle cyber terrorism, which poses a threat to all nations, could be this first step. If states can work together towards the attribution of terrorist operations to terrorist groups within cyberspace, we can work towards a proof of concept that concrete attribution is possible and we can work towards a reduction and possible elimination of anonymity within the space. Once this collaboration proves to be fruitful, the step towards collaboration to attribute cyberspace operations might be easier to take.

Progress in answering these questions in a legal context will enable the development of enforceable international laws within this space. Although this short discussion on the two critical questions identified within this paper is far from complete, it provides an initial step into how they might be answered and a potential first concrete step in the right direction. To achieve a complete answer, further discussions with experts in all fields, such as law, international relations, political science and computer science, have to occur. If the world wants to achieve regulation within this space, not one aspect can be left outside of the conversation. Otherwise, we can, again, go through the path of proposing legislation that actually reduces overall security within society rather than make society safer from cyber operations. Achieving regulation of this space should be a top priority of policymakers as the world becomes more digital every single day, and initiatives such as the Metaverse are being accelerated and have become the focus of some of the biggest technology companies. If regulation does not exist when people start interacting more in a virtual world where they can live, work, shop and do much more, we will be at the mercy of big tech firms as nations will fail to grasp hold of these worlds and we will be open to even more disruption from actors such as other nations and terrorist organisations.

Conclusion

Throughout this study, numerous facets of cyberspace have been explored, commencing with a comprehensive analysis of existing cyberspace regulations and endeavours to apply international law within this domain. Subsequently, the research delved into both warfare and terrorism manifested in cyberspace, demonstrating the crucial role it plays in contemporary society and the profound repercussions of any disruption. The latter sections elucidated the proponents of cyberspace regulation and its ramifications on international security, revealing that the absence of regulation in cyberspace yields both advantageous and detrimental outcomes for security. Where the ease of cyber espionage can lead to a greater level of trust within the international community, it also opens us up for more threats such as unreported vulnerabilities.

However, it is important to note that cyber espionage is not the sole operation executed in cyberspace. Examining the Ukrainian energy system attacks offers insights into alternative ways cyberspace can be exploited and the potential consequences. Additionally, the susceptibility of critical democratic processes, such as elections, to tampering is important to consider. Moreover, the transformation of TOR from a tool to keep people safe and advance human rights to a predominantly criminal-associated entity underscores the far-reaching implications for society and its security. Because of these aspects, the main conclusion of this paper has to be that cyberspace regulation is necessary for international security. The threats that many of our systems face due to their connectivity are immense. These threats further pose risks to our societies and way of life. Cyber security becomes even more critical given the ease for someone on the other side of the planet to hack into certain systems. Contemporary society faces risks due to actions made by States that were traditionally outside our sphere of influence and actors such as terrorists fighting a fight far outside our borders. Any cyber war can quickly turn into a new world war. Every action of cyber terrorism can lead to consequences felt by citizens that have no place in the conflict. To achieve international security, there needs to be international collaboration to tackle the threats within cyberspace and achieve regulation within the space to protect the citizens. The formation of international public-private partnerships will be crucial in facilitating the exchange of expertise on cyber security strategies, investigations, and threat intelligence. As anonymity enhances the appeal of cyberspace operations, efforts to reduce it without jeopardising societal security are essential. As data passes through infrastructure based in different countries and organisations the only way to deal with this anonymity safely is the cooperation to make it easier to establish the origin of the activity. This is the key to solving the problem, as not knowing what is transmitted due to techniques such as encryption is not the issue when talking about attribution as we want to establish where activity is coming from. Therefore we need to be able to link all the segments together to solve the puzzle and get closer to the root cause.

As cyber war looms, the fifth military domain will be utilised not only by States but also by terrorists and even private citizens. A single act, by a single actor, in cyberspace can plunge nations or the entire world into turmoil. The growing focus on virtual worlds exacerbates the inadequacy of current regulations, allowing nations to pursue increasingly strategic objectives. If governments continue to exploit cyberspace without pursuing regulation and cooperation, non-state actors will gain an advantage. Despite the numerous benefits that cyberspace provides, it also presents significant challenges that must be addressed by the international community. How we mitigate these is a question that has to be asked and answered within the international community. When this question is answered, both international and national security will benefit from it. Due to increased interconnectivity and collaboration on an international scale, national security cannot be achieved without considering international security. A coherent regulatory framework for cyberspace usage is needed to resolve issues such as anonymity. Swift action is necessary to initiate regulation, after which further efforts can be devoted to preventing nations from leveraging cyberspace for strategic objectives, both offensive and defensive. Additionally, responses to cyberattacks or the imposition of embargoes can be carried out legitimately and with human rights considerations. The most pressing question, however, is whether meaningful steps towards regulation will be taken before it is too late.

Ultimately, the effectiveness of cyberspace regulation will depend on the ability of governments and organisations to work together to address the complex challenges it presents. The stakes are high, as the potential consequences of failing to establish a robust regulatory framework can be catastrophic, and the effectiveness of cooperation between governments will be vital. As technology advances and the integration of cyberspace into every aspect of our lives deepens, it becomes increasingly important to find a balance between the benefits of connectivity and the need for security. An essential aspect of this effort will be promoting transparency, accountability, and trust among all stakeholders, including governments, private sector organisations, and individual users. This will require ongoing dialogue and cooperation, as well as the sharing of best practices, resources, and expertise. It is crucial that all parties recognise the shared responsibility they hold in ensuring the safety and stability of cyberspace. Moreover, striking the right balance between security and privacy will be a critical component of effective regulation. While monitoring and controlling malicious activities is important, it is equally important to protect the fundamental rights of individuals, including their right to privacy and freedom of expression. This delicate balance will necessitate a nuanced and thoughtful approach guided by the principles of international law and human rights.

In conclusion, the development and implementation of comprehensive cyberspace regulation is a pressing and complex challenge, requiring the concerted efforts of the international community. As nations and individuals become increasingly reliant on cyberspace, the need to address its inherent risks and vulnerabilities will only grow more urgent. Through collaboration, transparency, and a commitment to preserving both security and human rights, it is possible to create a regulatory framework that safeguards the integrity of cyberspace while allowing its users to continue reaping its many benefits. The first step towards the creation of this framework could lie in the area of cyber terrorism, where collaboration to achieve attribution and reduction of anonymity will be beneficial for all nations involved. The ultimate question remains: will the international community be able to act decisively and in unison before the consequences of inaction become irreversible? The answer to this question will have a profound impact on the future of cyberspace, international security, and the well-being of societies around the world.

About the Author

Sam Maesschalck is a researcher at Lancaster University and part of the Security Lancaster Research institute. His main research focuses on technical (systems and networks) and non-technical (cyberspace and international relations) aspects of cyber security, mainly focused within a critical infrastructure environment.

References

Abbate J (2000) *Inventing the internet.* MIT press.

Andrew L et al. (2020) The vulnerability of vital systems: how'critical infrastructure'became a security problem. In: *Securing 'the Homeland'*. Routledge, pp. 17–39. DOI:https://doi.org/10.4324/9780203926529-2.

Arquilla J and Ronfeldt D (1993) Cyberwar is coming! *Comparative Strategy* 12(2): 141–165. DOI:https://doi.org/10.1080/01495939308402915.

Assaf A and Moshnikov D (2020) Contesting sovereignty in cyberspace. *International Cybersecurity Law Review* 1(1): 115–124. DOI: https://doi.org/10.1365/s43439-020-00004-5.

Bancroft A and Scott Reid P (2017) Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society* 20(4): 497–512. DOI:https://doi.org/10.1080/1369118X.2016.1187643.

Banerjee M, Lee J and Choo KKR (2018) A blockchain future for internet of things security: a position paper. *Digital Communications and Networks* 4(3): 149–160. DOI:https://doi.org/10.1016/j.dcan.2017.10.006.

Baxter DJ (2017) E-governance and e-participation via online citizen budgets and electronic lobbying: promises and challenges. *World Affairs* 180(4): 4–24. DOI:https://doi.org/10.1177/0043820018771137.

BBC (2018) Russia 'meddled in all big social media' around us election. URL `https://www.bbc.co.uk/news/technology-46590890`.

Blaze M, Braun J and Advisors CG (2017) Defcon 25 voting machine hacking village. *Proceedings of DEFCON, Washington DC* : 1–18.

Bowie NE and Jamal K (2006) Privacy rights on the internet: self-regulation or government regulation? *Business Ethics Quarterly* : 323–342DOI:https://doi.org/10.5840/beq200616340.

Brill A (2015) The use of internet technology by cyber terrorists & cyber criminals: The 2014 report. DOI:10.3233/978-1-61499-528-9-1.

Bruderlein C (2009) Manual on international law applicable to air and missile warfare. *Bern, Switzerland: Harvard University Program on Humanitarian Policy and Conflict Research* DOI:https://doi.org/10.1017/CBO9781139525275.

Burt T (2021) New nation-state cyberattacks. URL `https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/`.

Buzan B, Hansen L et al. (2009) *The evolution of international security studies.* Cambridge University Press. ISBN 9780521872614.

Cha VD (2000) Globalization and the study of international security. *Journal of Peace Research* 37(3): 391–403. DOI:https://doi.org/10.1177/0022343300037003007.

Clarke RA and Knake RK (2014) *Cyber war.* Tantor Media, Incorporated Old Saybrook. ISBN 978-0-06-199239-1.

Collier K (2021) 50,000 security disasters waiting to happen: The problem of america's water supplies. URL `https://nbcnews.to/3gKzJ7G`.

Dannreuther R (2014) *International security: The contemporary agenda*. John Wiley & Sons. ISBN 978-0-745-65377-8.

Derbyshire R, Green B and Hutchison D (2021) "talking a different language": Anticipating adversary attack cost for cyber risk assessment. *Computers & Security* 103. DOI:https://doi.org/10.1016/j.cose.2020.102163.

Derbyshire R, Green B, Prince D, Mauthe A and Hutchison D (2018) An analysis of cyber security attack taxonomies. In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 153–161. DOI:https://doi.org/10.1109/EuroSPW.2018.00028.

Doswald-Beck L (1995) *San Remo manual on international law applicable to armed conflicts at sea*. Cambridge University Press. DOI:https://doi.org/10.1017/CBO9780511622052.

Easley LE (2014) Spying on allies. *Survival* 56(4): 141–156. DOI:https://doi.org/10.1080/00396338.2014.941545.

Farwell JP and Rohozinski R (2011) Stuxnet and the future of cyber war. *Survival* 53(1): 23–40. DOI:https://doi.org/10.1080/00396338.2011.555586.

Fitzmaurice GG (1956) The foundations of the authority of international law and the problem of enforcement. *The Modern Law Review* 19(1): 1–13.

Ghappour A (2017) Searching places unknown: Law enforcement jurisdiction on the dark web. *Stanford Law Review* 69: 1075. DOI:http://dx.doi.org/10.2139/ssrn.2742706.

Goldschlag DM, Reed MG and Syverson PF (1996) Hiding routing information. In: *International workshop on information hiding*. Springer, pp. 137–150. DOI:https://doi.org/10.1007/3-540-61996-8_37.

Harris S (2014) @ *War: The rise of the military-internet complex*. Houghton Mifflin Harcourt. ISBN 9780544251793.

Johnson DR and Post D (1996) Law and borders: The rise of law in cyberspace. *Stanford Law Review* : 1367–1402DOI:https://doi.org/10.2307/1229390.

Khan R, Maynard P, McLaughlin K, Laverty D and Sezer S (2016) Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In: *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*. pp. 53–63. DOI:https://doi.org/10.14236/ewic/ICS2016.7.

Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG and Wolff S (2009) A brief history of the internet. *ACM SIGCOMM Computer Communication Review* 39(5): 22–31. DOI:https://doi.org/10.1145/1629607.1629613.

Lenz H (2018) Achieving effective international cooperation: How institutional formalization shapes intergovernmental negotiations. *World Affairs* 181(2): 161–180. DOI:https://doi.org/10.1177/0043820018791644.

Leswing K (2020) Apple's fight with trump and the justice department is about more than two iphones. URL `https://www.cnbc.com/2020/01/16/apple-fbi-backdoor-battle-is-about-more-than-two-iphones.html`.

Liang CS (2017) Unveiling the" united cyber caliphate" and the birth of the e-terrorist. *Georgetown Journal of International Affairs* : 11–20.

Lukasik S (2010) Why the arpanet was built. *IEEE Annals of the History of Computing* 33(3): 4–21. DOI:https://doi.org/10.1109/MAHC.2010.11.

Maesschalck S, Giotsas V, Green B and Race N (2022) Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. *Computers & Security* 114. DOI:https://doi.org/10.1016/j.cose.2021.102598.

Maesschalck S, Staves A, Derbyshire R, Green B and Hutchison D (2023) Walking under the ladder logic: Plc-vbs: a plc control logic vulnerability scanning tool. *Computers & Security* 127: 103116. DOI:https://doi.org/10.1016/j.cose.2023.103116.

Maurer T (2018) *Cyber mercenaries*. Cambridge University Press. ISBN 9781107127609.

McCormick T (2013) The darknet. *Foreign Policy* (203): 22.

Miller T, Staves A, Maesschalck S, Sturdee M and Green B (2021) Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection* : 100464DOI:https://doi.org/10.1016/j.ijcip.2021.100464.

Mirea M, Wang V and Jung J (2019) The not so dark side of the darknet: a qualitative study. *Security Journal* 32(2): 102–118. DOI:https://doi.org/10.1057/s41284-018-0150-5.

Mueller ML (2020) Against sovereignty in cyberspace. *International Studies Review* 22(4): 779–801. DOI:https://doi.org/10.1093/isr/viz044.

NCSC (2021) Uk and allies hold chinese state responsible for pervasive pattern of hacking. URL https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking.

Olson P (2013) *We are anonymous*. Random House. ISBN 978-0434022083.

Price ME, Verhulst SG and Verhulst S (2005) *Self-regulation and the Internet*. Kluwer Law International BV. ISBN 9789041123060.

Reuters (2021) U.s. spied on merkel and other europeans through danish cables - broadcaster dr. URL https://reut.rs/35gt9z9.

Rid T (2012) Cyber war will not take place. *Journal of strategic studies* 35(1): 5–32. DOI:https://doi.org/10.1080/01402390.2011.608939.

Ritchie R (2019) Maersk: Springing back from a catastrophic cyber-attack. URL https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

Schmidt A (2013) The estonian cyberattacks. *A fierce domain: Conflict in cyberspace, 1986 to 2012* : 174–193.

Schmitt MN (2010) Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. In: *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, volume 151. ISBN 0-309-16086-3, pp. 163–64.

Schmitt MN (2017) *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. DOI: https://doi.org/10.1017/9781316822524.

Senger DE and Edmondson C (2019) Russia targeted election systems in all 50 states, report finds. URL https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

Shehod A (2016) Ukraine power grid cyberattack and us susceptibility: Cybersecurity implications of smart grid advancements in the us.

Sutton HI (2021) Positions of two nato ships were falsified near russian black sea naval base. URL https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.

The White House (2021) Executive order on improving the nation's cybersecurity. URL https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

UN General Assembly (2021) Open-ended working group on developments in the field of information and telecommunications in the context of international security .

United Nations (2016) The promotion, protection and enjoyment of human rights on the internet. URL https://digitallibrary.un.org/record/845728?ln=en.

United Nations (2021) Report of the group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security. URL https://www.un.org/disarmament/group-of-governmental-experts/.

US Senate (2019) Report of the select committee on intelligence united states senate on russian active measures campaigns and interference in the 2016 u.s. election volume 1: Russian efforts against election infrastructure with additional views. URL https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

Vera A, Lynch J and Carrega C (2021) Someone tried to poison a florida city by hacking into the water treatment system, sheriff says. URL https://cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison.

Volpicelli G (2021) The home office is preparing another attack on encryption. URL https://www.wired.co.uk/article/uk-encryption-facebook-home-office-nspcc.

Wicker SB (2020) The ethics of zero-day exploits— the nsa meets the trolley car. *Communications of the ACM* 64(1): 97–103. DOI: https://doi.org/10.1145/3393670.