GLOBAL RISK INTEL

Risk Report

ASSOCIATED RISKS AND LEGAL LIMITATIONS OF CYBER WARFARE

STRATEGIC | OPERATIONAL | FINANCIAL | COMPLIANCE

www.globalriskintel.com

DISCLAIMER:

THE VIEWS EXPRESSED IN THIS DOCUMENT ARE THE SOLE RESPONSIBILITY OF THE AUTHOR(S) AND DO NOT NECESSARILY REFLECT THE VIEWS OF GLOBAL RISK INTELLIGENCE. THIS DOCUMENT IS ISSUED WITH THE UNDERSTANDING THAT IF ANY EXTRACT IS USED, THAT BOTH THE AUTHOR(S) AND GLOBAL RISK INTELLIGENCE SHALL BE CREDITED, PREFERABLY WITH THE DATE OF THE PUBLICATION. THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE.

COPYRIGHT © GLOBAL RISK INTELLIGENCE. ALL RIGHTS RESERVED.

ASSOCIATED RISKS AND LEGAL LIMITATIONS OF CYBER WARFARE

RISK REPORT

Global Risk Intelligence

OCTOBER 30, 2019

Washington, D.C. · London · Dubai · Singapore

www.globalriskintel.com

PUBLIC RELEASE

Author

Yasemin Zeisl is a Risk Analyst at Global Risk Intelligence. She earned her MSc in International Relations and Affairs from the London School of Economics and Political Science (LSE).

Summary

State governments and private businesses are increasingly vulnerable to harmful cyber operations. The scope and versatility of cyberattacks indicate that they could become a key component of warfare in the future. While domestic laws on data privacy may protect consumers, international law lacks a comprehensive treaty on cyber warfare. Such a treaty would resolve ambiguities regarding the attribution of cross-border attacks, self-defense options, and the use of force. This risk report identifies key areas that are particularly vulnerable to international cyberattacks and offers various recommendations for improved cybersecurity initiatives.

Contents

1. Introduction:

The world's digital network is ever-expanding. Every year, more people benefit from technological innovation. The number of internet users worldwide has grown significantly since the 1990s. Almost 50% of the world population was connected to the internet in 2017, according to data records by the World Bank[1]. Digital permeation and technological advancement offer numerous benefits, but they also entail various risks. Cyberattacks have multiplied in recent years and are now a major threat to public and private institutions. Governments, businesses and individuals need to ensure that their data is safely processed and stored.

Technology transforms society in various ways. A key area that has been affected by such change is the conduct of war. War can now be waged in the digital realm: a cyber war can be carried out alone or in combination with physical attacks. Cyberattacks assume many forms and are commonly a component of asymmetric warfare – that is, a conflict between opponents with different military capabilities. States and non-state actors such as terrorist groups, insurgents, and hacktivists frequently engage in asymmetric cyber warfare. In some cases, state-sponsored hackers execute attacks against foreign states. The North Korean government, for instance, funds and controls groups of cyber specialists that infiltrate overseas networks to disrupt cryptocurrency exchanges. Other examples include accusations against Russia's government for manipulating the 2016 US presidential election and the 2017 Brexit referendum in the United Kingdom.

Cyber warfare not only presents physical challenges for a state's defense programs, but also raises intellectual questions that affect national security. While legal regulations provide security, lawmakers often find it difficult to keep up with the rapidness and adaptability of technological development. The nature and ramifications of cyber warfare create uncertainties for lawmakers that will need to be clarified. Establishing a precise definition of cyber warfare is a useful start for governments, international organizations, and lawmakers. Precise definitions will offer better insight into various types of threat and their extent. It is vital to pinpoint how severe, invasive, immediate, or measurable a cyberattack is. The role of states in a transborder attack and the military

[1] **World Bank (2017): *Individuals using the internet (% of population)*. Available at: https://data.worldbank.org/indicator/it.net.user.zs (Accessed: June 7, 2019).**

PUBLIC RELEASE

quality of a cyber invasion can determine appropriate preventive action and countermeasures against cybersecurity risks[2]. If decision-makers do not know what kind of risk they are encountering, enforcing suitable strategies against cyberattacks may prove difficult. Faulty assessment of a risk situation could lead to highly unfavorable results. Such outcomes include the disruption of national economies, political turmoil brought about by manipulated elections, espionage, or widespread private data theft.

The threat of cyberattacks lies in their invisibility. Compared to conventional armed military strikes, which leave behind physical destruction, cyber damage is less apparent to the public. Despite their inconspicuousness, cyberattacks can cause severe devastation. Particularly vulnerable industries and institutions are government bodies, the military, the financial sector, and critical infrastructures such as the energy industry, public health institutions (hospitals, etc.), or public transport systems.

2. A Definition of Cyber Warfare

Ever since Russian hackers attacked the servers of Estonia's government in 2007 and caused severe non-physical harm, international conflict has entered the new battleground that is cyberspace. The word cyber warfare is increasingly utilized in the media and the academic discourse. Definitions of the term are diverse and sometimes inconsistent. A central question is whether previous attacks have reached the scale of a war. One could argue that they are merely individual instances of aggression that do not compare to the extent of a war. Comparing cyber warfare and conventional warfare on land, by sea, or in the air is a difficult task. Conventional wars result in physical damage. Cyber war, in contrast, is less apparent and harder to anticipate. Attacks can be quick, and aggressors frequently remain anonymous. Despite their invisibility, large-scale cyber operations can result in the same level of damage as kinetic attacks. In some cases, cyber warfare may even cause greater destruction than conventional arms and armies.

Cyber warfare as defined by Martin Libicki can be divided into two categories. These are strategic and operational cyber warfare. The former is "a campaign of cyberattacks one entity carries out on

[2] **Schmitt, M. N. (n.d.): The law of cyber warfare: Quo vadis?, *Stanford Law & Policy Review* 25(269), p.280.**

another"[3]. The operational type "involves the use of cyberattack on the other side's military in the context of a physical war"[4]. Therefore, cyber warfare can be entirely digital or compliment physical warfare. Tactics of cyber warfare can be utilized in international and domestic conflicts. In the case of an international conflict, answers to legal questions often hover in a gray area.

Parties in a cyber war can be state governments as well as non-state actors that are covertly backed by foreign governments. Countries that are central players in cyber warfare are the United States, Russia, China, Iran, North Korea, and Israel. Ascribing the activities of hacking groups to a certain government can pose a complex problem to attacked states. Cyber terrorism often tends to be part of a government strategy that is meant to stay hidden. Hence, cyberattacks can be more than just isolated instances. They fit into larger foreign policy schemes of states.

2.1. Offense

Offensive cyberattacks are a comparatively convenient form of warfare. They are less costly than physical military operations, often require fewer personnel, and are relatively safe for hackers who operate from hidden, remote places. Therefore, cyber operations are particularly useful for warfare between forces of asymmetric strength.

Cyber attackers can resort to various tools of warfare. This includes sabotage through denial-of-service attacks or disruptions of critical infrastructures such as energy supply. Espionage or dispersion of propaganda are other forms of cyber offense. Tailored propaganda on social media platforms aims to influence the opinions of voters, and data analytics software is a powerful tool to perform this task. Russia has been previously accused of election manipulation, which is why the European Union (EU) was particularly vigilant in the months leading up to the European Parliament Election in late May 2019[5]. Another cyber espionage technique hostile groups or individuals may utilize is phishing. Fake emails allow attackers to spy on users. Hackers can unlock access to private

[3] **Libicki, M. C. (2009): *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND, p. 8.**
[4] **Ibid.**
[5] **Silva, M. (2019): Is Russia trying to sway the European elections?, *BBC*. Available at: https://www.bbc.com/news/blogs-trending-48296557 (Accessed: June 11, 2019).**

data through emails which direct users to malware-laden websites. This method is called spear phishing.

Cyberattacks which aim to monitor data traffic patterns, intercept data flows, or install corrupt data on a system are particularly harmful because of the extensive damage they inflict. Offensive attacks become especially critical when they are conducted against satellites, landlines, ground stations, or terminals which globally connect users. The consequence of operations with malicious intent can be large-scale data loss, data theft, disruption, denial of service, seizure of control over a satellite, or destruction of a satellite[6].

2.2. Defense

US President Donald Trump announced in mid-2018 that he aims to train and deploy a space force[7]. As outer space becomes increasingly militarized states such as the US, China, Russia, and India enhance their assets in space. Installing a national cyber force and employing cyber counterintelligence specialists would therefore compliment such militarization efforts. Considering that cyberattacks are a more immediate risk than a physical war in outer space, policymakers should make the training and deployment of a national cyber force a priority. A cyber force could protect government assets against foreign intervention on Earth as well as satellites in space. Japan has already made plans to create a cyber defense unit by 2023 as part of its ongoing national militarization endeavor[8].

A newly established cyber force would rely on financial and logistical support as much as on highly skilled professionals. In order to create an efficient force, military strategists should work closely with programmers and technology professionals who will execute operations. The success of such a

[6] See Harrison, T. et al (2019): Space Threat Assessment 2019, *International Institute for Strategic Studies*. Available at: https://www.csis.org/analysis/space-threat-assessment-2019 (Accessed: June 5, 2019).

[7] Dopp, T. (2018): Trump wants 'space force' added to military as new U.S. service, *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2018-06-18/trump-s-nasa-moon-shot-may-start-with-robots-before-astronauts (Accessed: June 8, 2019).

[8] Center for Strategic and International Studies (2019): Japan's defense strategy, *Center for Strategic and International Studies*. Available at: https://www.csis.org/analysis/japans-national-defense-strategy (Accessed: May 19, 2019).

PUBLIC RELEASE

force is highly dependent on well-trained hackers. Moreover, government agencies must cooperate with the technology sector to achieve goals. If these two vie with each other for contracts, defense objectives may not be realized, and states would remain vulnerable to cyberattacks. As a result, the state defense department may not be able to minimize damage, recover in time, or launch counterstrikes. Previously, technology giants such as Google and Microsoft have competed with government institutions such as the US Defense Department or the US Immigration and Customs Enforcement over contracts[9]. Once decision-makers understand the risk that cyberattacks pose to a state's national security, they should take first steps to defend users, institutions, and businesses within their cyberspace.

2.3. Cyber Peace

Cyber peace is a term that requires clarification. Numerous hurdles must be overcome in order to attain peace in a conventional war. In comparison, cyber peace may be even more difficult to realize. In cyber war, anyone competent enough to launch an attack can continue the war. Striking peace deals with fragmented, decentralized non-state groups defending diverse interests presents a complex challenge to heads of state. This is because there are no formal rules of diplomacy as in war between states. Furthermore, hackers often remain anonymous and their location of operation may change frequently. Therefore, cyber peace will be in the hands of state governments. They will have to take responsibility for actions carried out from within their sovereign territories. International law can be a tool to solve issues of accountability, but numerous legal questions remain unanswered since there is no international treaty on rules of engagement in a cyber war. National laws and existing international laws may provide some answers, but they do not cover all legal problems arising in cyber warfare. This is because the nature of cyber warfare differs from conventional warfare.

[9] Wheeler, T. (2018): In cyberwar, there are no rules, *Foreign Policy*. Available at: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ (Accessed: June 5, 2019).

3. The Nature of Cyber Warfare

There is a number of salient characteristics of cyber warfare that presents challenges to targets, victims, and policymakers. Creating awareness of the nature of cyberattacks may bring clarity on how to proceed with cybersecurity plans in the future.

The scope of cyberattacks varies greatly. While some cyberattacks may harm a large region-specific network, some attacks can be highly targeted. Depending on the objective of the attacker, targets can be either masses of people or just a single individual. A victim could be one bank account holder out of many or a person of authority like a high-profile politician or a CEO.

Collateral damage must be anticipated in cyber warfare. In conventional wars, militaries need to calculate the collateral damage of an attack. Before the start of an operation, strategists have to assess to what degree civilians are endangered. Non-state actors such as anonymous hacking groups are not likely to adhere to such rules. They focus on achieving the goal rather than causing more damage than necessary. Collateral damage involving a large number of civilians thus appears inevitable in an era of cyber warfare.

Anonymity is a central challenge. Prosecuting criminal acts that were conducted across borders already poses a challenge to domestic and international courts. Facing an unidentifiable perpetrator further complicates the issue of accountability. Furthermore, distinguishing between a state-sponsored group with higher motives from independent hackers without a specific agenda may be difficult. A denial-of-service attack against a government website does not necessarily reveal the intent of the attacker. If neither the identity nor the motive of hackers can be ascertained, prosecutors will not be able to initiate legal proceedings.

Unpredictability is another major hurdle associated with anonymity. Technology drives military advancement forward. Hypersonic weapons that are faster than any other existing jet fighter or missile are currently in development. They make military strikes significantly less predictable. In comparison to such unpredictable physical weapons, imminent cyberattacks are even more incalculable. Cyber warfare is quicker and more clandestine than conventional war, which is why defense strategists need to become more agile and flexible.

Cyberattacks reduce reaction and decision-making times. As technology advances and attacks accelerate in speed, decision-makers must arrive at a conclusion in increasingly compressed timespans. This can evoke mistakes and flawed decisions which can result in suboptimal outcomes. At the same time, technological advancements are an advantage. Artificial intelligence systems can support decision-makers under pressure and improve results, as they rapidly process large amounts of information. National cyber forces could benefit from such artificial intelligence aid.

Underestimated targets create weak spots for states. Poorly maintained and undervalued industrial control systems, healthcare systems, or transportation networks are easy targets. While policymakers anticipate grand attacks such as a Cyber-Pearl Harbor, they tend to ignore numerous vulnerable spots that are less prominent[10]. Bolstering cybersecurity systems in these areas does not come without financial cost, but it stabilizes the defense against cyber risks on a national level.

4. Vulnerable Domains in Cyber Wars

Cyber war can affect different domains of a state. Highly vital domains sustain the prosperity and survival of a state. Economic volatility, political turbulence, or social issues resulting from cyber disruptions pose a risk to not only certain industries like the energy industry or the military complex but also to the wellbeing of a state in a more comprehensive way.

4.1. The Political Domain

The first domain is the political and encompasses the military industry. Cyberattacks that immobilize defense systems of a country are serious risk for states, particularly if the attack is a planned offensive operation that is combined with a missile strike. Tools of cyber warfare enhance physical attacks. Cybersecurity must therefore prevent such a twofold risk. Another way in which the political realm can be affected is through the manipulation of public opinion. Cases such as the UK's departure from the EU demonstrate that a country's political outlook can transform vastly in

[10] **Wheeler, T. (2018): In cyberwar, there are no rules, *Foreign Policy*. Available at: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ (Accessed: June 5, 2019).**

the long-term. Brexit not only influences financial, economic, and political matters but also travel, settling, and working regulations for citizens of the UK and the EU. In addition, Brexit turbulences also diminish the trust between UK and EU politicians in Brussels and corrode European integration. Therefore, this development bears long-term implications for Europe.

4.2. The Financial Domain

Finance is the second key domain. Banks, cryptocurrency exchanges, international currency funds, and development banks fall into this category. The finance sector is the backbone of a country. A stable economy and secured monetary funds are vital to consumers, firms, and states. The safer and more stable an economy is, the more a country can flourish. In 2019, the number of state-sponsored cyberattacks on banks beyond state borders are expected to increase[11]. Attacks executed in the name of a state follow a political agenda that is unlike temporary attacks by independent cyber criminals. Improving cybersecurity systems in the financial domain also enhances the national security of a state.

4.3. The Social Domain

Health care systems are central to the social domain. If access to patient records is denied, doctors in hospitals, clinics, or practices will be unable to perform surgeries or prescribe vital medication. A complete loss or disruption of patient data constitute an even worse scenario. Human lives directly depend on uninhibited access to files. As health care institutions rely increasingly on digital information and technology, cyber risks regarding the safety of patients rise. Robots that are sufficiently advanced to perform surgery should be included in cybersecurity considerations. Corrupt robots may prove to be more of a disadvantage than an advantage.

[11] **Moon, A. (2019): State-sponsored cyberattacks on banks on the rise: report, *Reuters*. Available at: https://www.reuters.com/article/us-cyber-banks/state-sponsored-cyberattacks-on-banks-on-the-rise-report-idUSKCN1R32NJ (Accessed: June 8, 2019).**

4.4. The Infrastructure Domain

Health care systems are central to the social domain. If access to patient records is denied, doctors in hospitals, clinics, or practices will be unable to perform surgeries or prescribe vital medication. A complete loss or disruption of patient data constitute an even worse scenario. Human lives directly depend on uninhibited access to files. As health care institutions rely increasingly on digital information and technology, cyber risks regarding the safety of patients rise. Robots that are sufficiently advanced to perform surgery should be included in cybersecurity considerations. Corrupt robots may prove to be more of a disadvantage than an advantage.

5. The Vulnerability of the Internet of Things

As electronic devices become increasingly interconnected, cybersecurity is confronted with manifold cybersecurity weak spots. The internet of things pervades an increasing number of households around the world. Smart devices that are connected to the internet extend from surveillance cameras or refrigerators to smart speakers like the Amazon Echo. The range of products that establish an interconnected digital network is broad. According to estimates, the number of 'internet of things' devices will rise to approximately 21 billion by 2020[12]. Such an enormous permeation of households and workplaces will become a major challenge to cybersecurity personnel because interconnected devices create a wider net of targets vulnerable to cyberattacks. An issue that must be addressed in this context is consumer protection. Many users may be unaware of potential cyber risks and give preference to convenience over safety.

A country that will be particularly vulnerable to cybersecurity risks in the future could be Japan. The country is planning to become a 'Society 5.0' which is based on the fundament of the internet of things. Even if such encompassing digitalization entails numerous benefits, risks for a society relying heavily on smart devices, artificial intelligence, and the internet should not be overlooked.

[12] **Stavridis, J. & Weinstein, D. (2016): The internet of things is a cyberwar nightmare, *Foreign Policy*. Available at: https://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/ (Accessed: June 5, 2019).**

Manufacturing companies also play a crucial role in cybersecurity matters. The country of origin of a business is a determinant in the perception of risks associated with a product. Chinese telecommunications firm Huawei has been struggling to export services and devices to western countries because of espionage allegations. The ongoing trade war and rivalry for power between China and the United States is the basis of mistrust towards Huawei. The US and Australia have banned Huawei entirely. European countries such as the United Kingdom and France aim for stricter regulations on Huawei products.

6. Cyber Warfare in Outer Space

Militarization of cyberspace coincides with the militarization of outer space. A closer look at the similarities between these two realms allows for a better insight into cyber warfare. Both cyberspace and outer space are strongly reliant on technology and can be utilized with the aid of technology only. Furthermore, both realms are internationally shared spaces. No country possesses sole sovereignty over cyberspace or outer space. This complicates issues relating to criminal accountability. At the same time, it is of imperative importance to provide clarity on legal questions since both spaces are key determinants in the international struggle for power.

Another point to consider is that technology connects cyber space and outer space. Cyberattacks against satellites affect an immense number of people globally. Therefore, they should be a focal constituent of cyber defense concerns. An attack against outer space assets results in massive financial losses, impairment of strategic resources, and reputational damage. Furthermore, cyberattacks that incapacitate satellites also create a blind spot in the physical defense of a country. States will not be able to track subsequent kinetic attacks. This is an alarming disadvantage. A war of this kind would find a conclusion relatively quickly. Victims of an attack of such a grand scale will not only be military personnel but also an enormous number of civilians. Therefore, bolstering cybersecurity in outer space is as vital to a thorough cyber defense strategy as securing cyberspace on Earth.

The cybersecurity program of the United States' National Aeronautics and Space Administration (NASA), for instance, relies on several components that assure the safety of data. These components

range from vulnerability assessments, security testing, risk evaluation and risk management to security training[13].

7. Cyber Warfare Laws

From a legal point of view, cyber warfare is full of ambiguities because there is no applicable international treaty. A central question, therefore, is whether domestic and international laws on physical warfare apply to the cyberspace as well. Answers to this question leave room for interpretation. Since the nature of cyberattacks differs from kinetic attacks, it is difficult to determine when the magnitude of a cyberattack is large enough to trigger the right to armed self-defense. Decisions to execute physical retaliation may be based on state interests rather than laws thus far. On May 5, 2019, Israeli forces conducted a physical attack against hackers of the Palestinian terror organization Hamas, inflicting casualties. This was the first time that a physical counterstrike was initiated while a cyberattack was in progress[14].

The issue of attribution is another challenge that needs to be resolved. Questions of attribution are largely concerned with how to manage uncertainty and sovereignty. A state can only be held responsible for a cyberattack if the attack can be attributed to state institutions. The complexity of attribution lies in the question of who executes an attack. Governments can commission non-state actors who are not affiliated with an official state organ to execute cyberattacks. This confronts courts with two problems. Firstly, if the individual or group responsible for the attack is unclear, courts cannot proceed. Secondly, even if non-state actors are identified, international law commonly does not hold states accountable for their actions[15]. The International Court of Justice acts as an arbiter only between states. In order to bring a state to the International Court of Justice,

[13] NASA (2017): *Cybersecurity services*. Available at: https://www.nasa.gov/centers/ivv/services/cybersecurity.html (Accessed: June 5, 2019).

[14] Hay Newman, L. (2019): What Israel's strike on Hamas hackers means for cyberwar, *Wired*. Available at: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/ (Accessed: June 5, 2019).

[15] Payne, C. & Finlay, L. (2019): International law cannot keep up with cyber-criminals, *World Economic Forum*. Available at: https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/ (Accessed: June 5, 2019).

PUBLIC RELEASE

it must be proven that the state government had effective control over a cyberattack by non-state actors within state territory. This means that the government must explicitly order an attack. Financial support or provision of equipment for hackers is not sufficient proof to assign responsibility to a state[16].

Article 2(4) of the United Nations Charter prohibits threats or the use of force against a foreign state because states possess sovereignty over their territory[17]. The use of force clause also applies to cyberspace. A state, however, can argue that self-defense against an armed attack justifies retaliation maneuvers. While cyberattacks can be highly destructive, damage oftentimes is not physical. Without a systematic categorization of cyberattacks that compares with physical equivalents it may prove difficult to declare a cyber offense as an armed attack. If the destructive force of a cyberattack officially matches a kinetic attack, then a state may argue that retributive self-defense is justified. Offering clarity and international standards on such complex questions will aid courts and targeted states in the future.

Even though some legal issues require interpretation, there are laws that provide answers. Domestic laws such as the *Espionage Act of 1917* of the United States or the *Official Secrets Act of 1911* and *1920* of the United Kingdom may offer clarity on cyber espionage issues. Regarding international laws, the 2001 *Budapest Convention on Cybercrime* by the Council of Europe sheds light on issues relating to copyright infringement, online fraud, and network security. This international treaty was signed and ratified by member states of the EU as well as several non-EU states including the US, Canada, Australia, Senegal, Turkey, Sri Lanka, and Japan[18]. Signatory states of the treaty are required to provide mutual assistance in the prosecution of cybercrimes. Article 32 of the convention also permits trans-border access to stored computer data with the consent of

[16] Payne, C. & Finlay, L. (2019): International law cannot keep up with cyber-criminals, *World Economic Forum*. Available at: https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/ (Accessed: June 5, 2019).

[17] United Nations (1945): *Charter of the United Nations, Article 2(4)*. Available at: http://legal.un.org/repertory/art2.shtml (Accessed: June 11, 2019).

[18] Council of Europe (n.d.): *Parties/Observers to the Budapest Convention and observer organisations to the T-CY*. Available at: https://www.coe.int/en/web/cybercrime/parties-observers (Accessed: June 11, 2019).

PUBLIC RELEASE

the data owner to facilitate investigations[19]. Thereby, the consent of state authorities can be circumvented. Russia's government strongly objects to this regulation, aiming for alternative solutions[20]. A transborder challenge that remains is the extradition of cybercriminals.

Another project to provide clarity on international cybercrime laws is the *Tallinn Manual on the International Law Applicable to Cyber Operations*. It is a non-governmental, non-binding examination of how international humanitarian law and laws of war apply to cyberspace. It was published in 2013 by legal experts in the field of cybercrime who are associated with the North Atlantic Treaty Organization (NATO). An updated version under the name *Tallinn Manual 2.0* is available since 2017. The manual categorizes cyberattacks according to their level of severity and defines what kind of cyberattacks classify as armed attacks. While the *Tallinn Manual* is a comprehensive study of the application of international law in cyber operations, it is not an international treaty. Therefore, it is not a binding contract with which states have to comply. The manual only offers guidance on future efforts to draft international laws on cyber warfare. A treaty on cyber war would supplement the Geneva Conventions which regulate humanitarian treatment in wars but lack sufficient clarity in matters relating to cyber warfare.

8. Cybersecurity Recommendations

The following points should be considered to ensure an adequate management of cybersecurity risks in a time of growing digitalization.

- An important first step for ensuring cybersecurity is defining the key terminology . This includes terms such as cyber war, cyber warfare, cybercrime, cyberattacks, and the right to self-defense. Authorities should differentiate between different degrees and types of risk. For instance, government policymakers should clearly map out when the extent of an attack is large enough to be categorized as national threat or when counterintelligence operations

[19] **Council of Europe (2001): *Budapest Convention on Cybercrime*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed: June 11, 2019).**

[20] **Tass (2018): Russia to propose draft cybersecurity convention to UN General Assembly, *Tass*. Available at: http://tass.com/politics/1011749 (Accessed: June 11, 2019).**

PUBLIC RELEASE

for the purpose of self-defense are appropriate. Clarity on such terms and questions does not merely serve intellectual purposes but it will also facilitate practical applications. Having knowledge of different risks and their impact will be useful in real-life situations. This promotes systematic and agile risk management. Reaching an international consensus on the terminology, however, is likely to take time and effort.

- A second step would be to establish a clear cybersecurity policy and strategy . This step is vital for further proceedings. Flawed policies and strategies can result in a faulty or imprecise execution. Policymakers, strategists, and technology experts should cooperate in this endeavor to produce optimal results.
- Installing a cybersecurity unit backed by the government to manage and evade risks could aid in safeguarding national security. A cybersecurity unit should consist of military strategists as well as programmers and cybersecurity experts to produce the best possible results. Strategist will map out plans, programmers will execute operations, and experts will review the process and results. Such a national cybersecurity force should be headed by a professional that possesses a proficient understanding of cybersecurity risks and strategic planning. This professional should cooperate with politicians of the highest ranks in order to adequately implement cybersecurity policies.
- The cooperation between government agencies and the technology sector can streamline cybersecurity programs. The practicability of this may be difficult, but it could further aid in managing risks and tailoring solutions.

Businesses and governments should not underestimate the importance of maintenance work. Filling cybersecurity gaps and vulnerable spots in a system takes effort, sufficient funding, experienced staff, and time. It is detail-oriented maintenance tasks rather than grand military strikes that will help to decrease cybersecurity risks. Planning for regular upgrades, routine checks, and cyberattack recovery guidelines is an essential step for companies and government institutions.

9. Concluding Thoughts

Cyberattacks are likely to become an increasingly frequent occurrence. Worldwide cyber operations such as the WannaCry ransomware attack in May 2017 are proof of how extensive cyber risks can be. Australia has been a victim of several cybersecurity breaches in recent years. In 2015, the Australian Bureau of Meteorology suffered a malware attack, and in 2018, computer systems of the Australian National University were invaded[21]. Other examples include malware attacks against electricity facilities and the finance and defense ministries in the Ukraine in 2016 and malicious cyber infiltrations of nuclear power plants in Iran in 2010[22]. The variety of potential targets and the versatility of attacks is broad. Potential targets range from political and financial establishments to social institutions and infrastructure. This is why cyber warfare poses a high risk to public institutions as well as private businesses. If systematically executed, cyberattacks can be categorized as a part of cyber warfare.

As digitalization advances and technological innovations penetrate society, cyberspace offers manifold, cost-effective opportunities for non-state actors such as insurgencies, terrorist groups, or hacktivists to wage war. In contrast to conventional warfare, cyber warfare requires comparatively little technological equipment. State militaries spend vast amounts of money to build up offense and defense capabilities. Non-state actors commonly do not possess such large financial means, which is why cyberspace is likely to become a progressively central battleground for non-state actors. At the same time, clandestine government-backed cyber operations against other countries complicate legal accountability because government involvement must be clearly proven.

Holding actors responsible for cybercrimes is also difficult because international treaties on cyber warfare have not been written yet. And even if a cyber warfare equivalent of the Geneva Conventions were composed, state authorities would have to sign and ratify such treaties.

---

[21] Payne, C. & Finlay, L. (2019): International law cannot keep up with cyber-criminals, *World Economic Forum*. Available at: https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/ (Accessed: June 5, 2019).

[22] Keating, J. (2011): Report: Stuxnet could cause Iranian 'Chernobyl', *Foreign Policy*. Available at: https://foreignpolicy.com/2011/01/31/report-stuxnet-could-cause-iranian-chernobyl/ (Accessed: June 5, 2019); Zinets, N. (2016): Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar', *Reuters*. Available at: https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC (Accessed: June 5, 2019).

PUBLIC RELEASE

Governments that rely on cyberattacks as a tool of war are not expected to agree to such an international treaty. The right to sovereignty further implicates that states are not obligated to submit to an international treaty. Therefore, private firms and public institutions need to understand the nature of cyber warfare and improve cybersecurity measures to prevent damage which cannot be prosecuted with the tools of international law. Complete safety cannot be guaranteed. Systematizing security options, however, can decrease risks and limit damage.

www.globalriskintel.com