GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

WORKING PAPERS

Societal Risks and Potential Humanitarian Impact of Cyber Operations

PIA HÜSCH AND HENNING LAHMANN

JUNE 2022

THE GENEVA ACADEMY A JOINT CENTER OF
GENEVA GRADUATE INSTITUTE
INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES
UNIVERSITÉ DE GENÈVE
FACULTY OF LAW

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Private and state cyber actors have become increasingly skilled and sophisticated. States' activities in cyberspace have been seen as a return to "great power competition". They often outsource their cyber operations to proxy actors acting on their behalf, thereby outsourcing the work and some of the risks. Independent private actors largely consist of cyber criminals, acting mostly out of financial motives. Their activities have increased in sophistication, establishing a lucrative and wide-ranging black market for data as well as services.

2. A number of trends can be identified with respect to the methods of adversarial cyber operations. These include an increase in self-propagating malware and reconnaissance operations; increased bypassing of two-factor authentication; the use of artificial intelligence in offensive cyber operations; information operations (e.g. for the creation of deep fakes). ; and the professionalisation of the black market.

    a. Especially ransomware attacks have become more sophisticated, often directly targeting certain companies and institutions; moreover, the threat to publish data stolen during such activities has become more frequent.

    b. Information operations raise particular concern; however, they remain difficult to define and also differ from cyber operations in important respects, which render the problem of addressing them more than a simple cyber security issue.

    c. Supply chain attacks pose significant risks and particularly concern high-tech companies and software development companies.

    d. Cyber operations in support of traditional military operations during armed conflict have been employed by a number of countries in recent years. Similar to operations during peacetime, they have the general purpose of intelligence gathering and disruption. They however potentially bear more severe consequences for the civilian population than peacetime operations as the nature of conflict may lead military decision-makers to proceed with less caution. Furthermore, the civilian population relies on civilian infrastructure, which may be more vulnerable than military systems and thus make for attractive targets of cyber operations, whether lawful or not.

3. Cyber operations may have a great variety of different objectives and are especially concerning where they are directed against an entire society or aim at decreasing trust in societal institutions. Although operations against a whole society, e.g. by disrupting essential services and infrastructure over a sustained period of time, are difficult to carry out, operations targeting trust may be highly effective and difficult to mitigate. Operations against physical objects have occurred less frequently to date.

4. The impact of cyber operations depends largely on the target's vulnerabilities, and of the consequences of disrupting such a target. The private sector is most vulnerable where digitalisation happened quickly and without necessary precautions or if the associated cyber security infrastructure is underdeveloped and/or underfunded. Similar considerations apply to the public sector and critical infrastructure. A society's vulnerability as a whole largely depends on its level of technology integration, as increased interconnectivity heightens the risk of more severe impact caused by cyber incidents. Increased vulnerability of a society occurs where it is particularly dependent on one technology or where certain types of critical infrastructure represent single points of failure.

5. The Covid-19 pandemic serves as an example of how external factors can influence and impact societal risks and vulnerabilities posed by cyber operations. It has largely increased risks e.g. by advancing digitalisation at a rapid speed, often without companies sufficiently preparing for the risks posed by increased digitalisation. It has also shown how vulnerable public healthcare is both in view of adversarial cyber conduct and disinformation campaigns.

6. The impact of cyber operations also depends on how resilient the target is. A number of measures can be taken in order to increase resilience.

   a. Steps can be taken to prevent adversarial cyber operations. This includes safety and security measures such as keeping software up to date as well as relying on state-of-the-art technologies such as AI-driven intrusion detection systems. An important factor is the creation of general awareness and the implementation of adequate cyber hygiene. International defence mechanisms and increased cooperation between public and private sector companies are further ways to improve cyber resilience.

   b. Other steps to increase resilience concern a society's susceptibility to disinformation campaigns. Where pupils are taught in media literacy early on, vulnerability decreases. Overall, a society becomes less vulnerable where the public is educated on cyber security and potential consequences and where emergency plans are implemented and disseminated ahead of any large-scale cyber security incidents.

   c. Attribution remains difficult and time-consuming despite capabilities generally having improved. The utility of attribution for the purpose of deterring hostile actors remains contested. In light of the observation that the credibility of attribution largely depends on who is making the claim, a neutral and independent, non-state fact-finding mechanism might be worth considering though challenging to establish.

Recovery can further attenuate the negative impact of cyber operations, which might involve a range of different measures, for instance regularly backing up data.

I .INTRODUCTION

This report is part of the “Digitalization of Conflict: Humanitarian Impact and Legal Protection” project a joint initiative between the International Committee of the Red Cross (ICRC) and the Swiss IHL Chair at the Geneva Academy of International Humanitarian Law and Human Rights. It aims to explore humanitarian consequences and protection needs caused by the digitalization of armed conflicts and the extent to which these needs are addressed by international law, especially international humanitarian law (IHL). The joint initiative adopts a multi-disciplinary perspective that takes into consideration the interrelated technical, military, ethical, policy, legal and humanitarian aspects to address three overarching questions:

1. What risks, potential humanitarian consequences, and protection needs for conflict-affected populations arise on the digital battlefield?

2. Does international law, in particular IHL, adequately address these risks and protection needs?

3. If not, what recommendations could be developed in terms of law and policy beyond the existing IHL framework to mitigate these risks and address these protection needs?

Focusing on some aspects of the first of these questions, two expert workshops and four other consultations with individual experts were held between February and May 2021. A range of eminent experts from different academic and practical backgrounds relevant to the subject matter from various parts of the world were invited. The workshops’ and consultations’ overarching objective was to provide an up-to-date assessment of existing risks and protection needs in light of contemporary and future military cyber capabilities. It built notably on earlier work by the ICRC on the topic.[1]

The present report presents the condensed outcome of these consultations. Addressed primarily to political decision-makers, academics, researchers, and lawyers, the report aims at providing an informed overview of the latest trends in international cyber security and conflict. To this end, it is divided into six interrelated parts. The first five each highlight and analyse recent relevant developments in order to address the key questions related to contemporary cyber conflict: (1) Who are the *actors* involved in adversarial cyber operations? (2) What *methods* do they use? (3) What are the *objectives* of such operations? (4) What do the *vulnerabilities* of the targets depend on? (5) What can be done to strengthen these targets’ *resilience* against cyber harm? A sixth, concluding part briefly touches upon some of the legal issues raised during the workshops that merit more in-depth consideration in the further course of the initiative.

II. ACTORS

The first issue to assess when it comes to cyber operations is the aspect of actors. Due to the structural features of cyber infrastructure, it is not always apparent who is carrying out cyber operations and to what ends. Various actors and their methods and motives can be distinguished, particularly state actors on the one hand and cyber criminals on the other, as well as the increasingly relevant category of proxy actors acting on behalf of states.

1.1. STATES

States are increasingly expanding their cyber capabilities. For some experts, states’ engagement in cyberspace signifies a return to “great power competition”, meaning that leading global powers have started to employ their cyber capabilities to try influencing the

[1] ICRC, The Potential Human Cost of Cyber Operations (Laurent Gisel and Lukasz Olejnik eds.), ICRC, Geneva, 2019; ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts (Ewan Lawson and Kubo Mačák eds.), ICRC, Geneva, 2021.

behaviour of other states. There is also a related trend of states implementing offensive cyber policies such as "defend forward" to persistently engage with their adversaries in cyberspace.[2] At the same time, some experts observed that, in a number of instances, states would have relied on proxies instead of acting directly through their own militaries or intelligence agencies (see section 1.2 below). State-of-the-art offensive cyber operations however require a considerable amount of expertise and resources, including highly qualified professionals, which somewhat limits the role of private actors regarding certain types of high-end activities.

There is also an increasing involvement of (civilian) intelligence agencies such as the CIA or GCHQ in (military) cyber operations. In part, this fact is a direct result of the important role that the activity of information gathering plays in the preparation of cyber operations. The involvement of such agencies further blurs the lines between military and civilian actors.

1.2. PROXY ACTORS

As mentioned, the workshop participants stressed that there are widespread claims of states relying heavily on the services of non-state actors that serve as proxies on their behalf, though such claims are contested. The types of specific tasks these actors are reported to engage in range from the development of exploits to the delivery of discovered vulnerabilities and the deployment of malware, i.e. the carrying out of entire offensive cyber operations. The sponsoring of such private entities provides states the opportunity to not only outsource the work involved but also some of the risks. Outsourcing may be attractive because attribution is difficult to establish with a sufficient degree of evidence, so it may enable the concerned state to eschew legal or political responsibility for its conduct. However, using proxy actors also carries risk, as they may have or develop their own motivations to engage in malicious cyber conduct, which may make them difficult to control by the state that employs them.

1.3. INDEPENDENT PRIVATE ACTORS

Purely private actors, i.e. non-state actors who do not serve as state proxies, differ from state actors in a range of characteristics. Most noteworthy is the fact that such actors frequently act for financial gain. Unlike states, this implies that they mostly do not pursue political objectives when carrying out offensive cyber operations.

Recently, some private actors have become increasingly sophisticated. One noteworthy mode of conduct that reflects the degree of professionalisation of cyber criminals is the growing practice of conducting so-called reconnaissance attacks with the aim of selling the obtained credentials of their victims on the dark web without exploiting them themselves. Information stolen in this way will often include login credentials, but also information on the vulnerability of IT systems as well as access to already infected systems. This type of actors can be described as "initial access brokers". This whole development has the effect of significantly increasing the speed and scale at which offensive cyber operations can be carried out.

To keep up with this increased professionalisation, cybersecurity and cyber defence need to intensify efforts. With a raising awareness for the need for better cyber security in the public as well as private sectors, more jobs are created, yet many of them cannot be filled given the lack of qualified and experienced applicants.[3]

The overall level of IT-related skills and technical knowledge required to carry out these cyber-criminal endeavours remains however relatively low. Some experts argued that cyber operations conducted by cyber criminals pose a greater risk to human life and

[2] See M.P. Fischerkeller and R.J. Harknett, Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation (2019) Cyber Defense Review 267.

[3] See e.g. William Crumpler & James A. Lewis, The Cybersecurity Workforce Gap, 29 January 2019, https://www.csis.org/analysis/cybersecurity-workforce-gap.

health than those driven by nation-states, as their targets are often civilian companies and individuals or because they are launched in a reckless and indiscriminate manner.

A further issue in relation to cyber security is the considerable threat posed by insider attacks. Despite the continuing proliferation of threat actors, law enforcement has generally made progress in terms of the identification of cyber criminals. As a result, more and more known criminal individuals are put on police watch lists, which severely restricts their ability to travel without the risk of being arrested.

III. METHODS

Given the speed at which technological advancements are made, cyber conflict is a rapidly developing area. Nevertheless, some trends relating to the methods used to carry out cyber operations are clearly distinguishable. Firstly, the use of so-called self-propagating malware such as worms and viruses has increased, and is the most prevalent method of attack against IT systems. It is significantly more widespread than other methods such as the use of trojans or password theft. As the name indicates, self-propagating malware has the ability to spread on its own from system to system and may in fact continue to do so even years after it had originally been deployed. Such malware therefore poses a sustained risk for a potentially long time. Most malware will be deleted in the process of reinstalling a computer's operating system, although there are some specimen that can withstand even such more radical measures.[4]

Conversely, the use of trojans – i.e. malware which masks as regular software but is planted on a target system for purposes of monitoring or other types of exploitation once it has been activated – has decreased. Secondly, there has been a surge in reconnaissance operations (see section 1.3 above). This is related to a third trend, which is the increased bypassing of two-factor authentication. For example, hackers may use the password reset function or bypass the second authentication step by using brute force to guess a four- or six-digit code. Fourth, the occurrence of large-scale data leaks vastly increased. Finally, the use of artificial intelligence is also on the rise, including in the conduct of offensive cyber operations and information operations (e.g. for the creation of deep fakes).

While cyber operations causing physical destruction remain rare, not least due to their complexity, the degree of sophistication should not be equated with the impact of an operation. To the contrary, harmful effects can also be achieved with cyber operations that lack any significant level of technical or operational sophistication.

It was noted that the (black) market has grown and professionalised significantly, and that it is too easy to acquire security-relevant data such as passwords, both legally and illegally, as much of the market is unregulated. One expert expressed the view that Western states subconsciously support such a market by accelerating a cyber arms race while at the same time leaving the market mostly unregulated. Rogue actors can access this market and use it to cause significant harm.

2.1. RANSOMWARE AND OTHER MALWARE

The perhaps most clearly identifiable trend is the continuing increase in ransomware attacks. Two main variants of this mode of offensive cyber operation can be distinguished. On the one hand, there are **opportunistic ransomware** operations conducted by using automated ransomware that spreads indiscriminately. On the other, more recently there has been an observable trend towards **targeted ransomware** activities that are directly controlled by human agents. Although targeted ransomware attacks are often more lucrative than opportunistic attacks, they may

[4] See Michael Kan, Suspected Chinese Hackers Unleash Malware That Can Survive OS Reinstalls, PC Mag, 5 October 2020, https://uk.pcmag.com/security/129035/suspected-chinese-hackers-unleash-malware-that-can-survive-os-reinstalls.

also be conducted for the purpose of political blackmailing as opposed to purely monetary incentives. They are also used where the target in question is especially difficult to access, as is the case with some highly specific, generally well-secured industrial control systems employed in critical parts of certain types of critical infrastructure such as power plants.[5]

In recent years, the gradual professionalisation of ransomware attacks has stood out, particularly with respect to reconnaissance activities for targeted operations. At the same time, there has been an increase in phishing attempts, and although these operations often do not carry any immediate consequences, they may lead to damage or other negative effects further down the line. In addition, the practice of double extortion has become more common in the context of stolen data. This means that apart from threatening to delete or alter data, data is “held hostage” while attackers threaten to leak the data unless ransom is paid. Such practices are increasingly applied to specifically targeted big companies and less frequently against opportunistic targets. These trends further implies that targeted operations are often prepared over the course of several months in advance to gather a sufficient amount of information during the preparatory stages. Another more novel aspect of the professionalisation of ransomware operations are so-called “breach as a service” offerings made on the dark web. Such services may provide different types of monetisation schemes; for example, hackers acting as “initial access brokers” may offer access to a target system to their customer instead of carrying out the entire ransomware operation on their own.

In addition to these cyber-criminal activities, ransomware operations can be used for military purposes. Military interest in such operation will usually not primarily lie with the monetary gain. Rather, states might have an interest to make it look like the ransomware operation was conducted by cyber criminals, thus using this mode of conduct primarily as a smoke screen to distract from other motives and to hamper attribution. Such operations may actually involve deleting data sets while causing an irreversible physical impact on the storage devices to decrease the chance for the victim to recover with backups or attacking back-up data centres directly by launching cyber operations against them.

2.2. INFORMATION OPERATIONS

Another significant trend is the increasing deployment of digitally-enabled information operations. Although information operations have always existed in some way or another, the extent to which the resort to digital means is capable of accelerating the effect and impact of information operations is concerning. This concern is exacerbated further by the recent developments to apply artificial intelligence technology to information operations, for example to create deep-fake videos. In principle, information operations do not require massive resources if compared to sophisticated cyber operations, although some variants may involve considerable resources that might not be available to every actor.

Difficulties arise both with respect to the question of how to define and identify “cyber-enabled information operations”. For example, consider the use of bots on social media; no agreement could be reached during the consultations as to whether such a case would fall under the definition of “cyber-enabled information operations”. For some experts, even traditional mainstream media organisations such as BBC or CNN, now able to reach vastly larger audiences online, can be considered as engaging in cyber-enabled information operations that exert influence on the internal affairs of other, particularly non-Western states.

Furthermore, the difficulty to define and to identify information operations implies that a

[5] It bears mentioning that not all critical infrastructures are per se difficult to access. In 2017, the UK national health system (NHS) was targeted on a large scale. The NHS used Windows 7 OS at the time, making it a relatively easy target. See National Audit Office, Investigation: WannaCry cyber attack and the NHS, 27 October 2017, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

successful defence strategy is more difficult to implement, as the key challenge here is not the technology used in itself but *how* it is used to spread information to humans. An additional factor to consider is the right to freedom of expression. Acting against the threat of information operations should proceed with caution so as to not unduly infringe on this human right.

It is important to note that information operations are conceptually different from other cyber operations as they target human psychology instead of computer systems or physical assets (see also sections 3.2 and 4.3 below). Not least due to this defining attribute, addressing information operations, whether or not accurately described as "cyber-enabled", is not a cyber security issue properly understood.

Finally, information operations can also play a significant role during armed conflicts, for example in support of traditional military operations. Experts voiced concern regarding the far-reaching and destructive effects information operations can have not only during active hostilities but also in post-conflict situations. In particular, information operations targeting the trust in society and institutions were regarded as a particular problem in this context (see section 3.2 below).

2.3. SUPPLY CHAIN ATTACKS

While offensive cyber operations against software and hardware supply chains remain a rather uncommon phenomenon, their occurrences increased recently. Such supply chain attacks are mainly carried out by way of infiltrating a target system through the product provided by a third party (e.g. a software or hardware provider) that legitimately enjoys access rights to the target system and its related data. This mode of malicious conduct causes concern due to its potentially devastating impact on the operations of high-tech companies, software development companies, as well as some critical infrastructure sectors such as the energy sector, particularly electricity or natural gas suppliers. More importantly, supply chain attacks often affect products which are used for monitoring and maintaining security across several companies. If a malicious actor manages to compromise the code base of the software used by several large companies (for instance an operating system or an industrial control system), this will gain the actor access to a number of targets at once. This renders the assessment of the impact difficult. In this context, the SolarWinds incident provides an alarming example, as it illustrates the far-reaching consequences that a supply chain attack can have.[6]

Aside from the immediate impact on the operations of affected institutions, supply chain attacks may have far-reaching negative systemic effects over the long term . Software and hardware supply chains rely on relationships of trust between vendors and their customers at the end of the chain – not only for the delivery of new products but especially also in regard to the necessary frequent software and system updates. As the frequency of supply chain attacks increases, this essential trust inevitably decreases, which risks compromising the entire existing system of supply chain infrastructure that both the private economy and public institutions rely on.

2.4. CYBER OPERATIONS IN SUPPORT OF TRADITIONAL MILITARY OPERATIONS

The possibility of a large-scale cyber-attack on a nation-wide level seems unlikely. In particular, the experts expressed doubts as to the ability to sustain such an attack over an extended period of time and a defined location in combination with the idea of impacting multiple systems at the same time. Nevertheless, it appears that certain cyber operations were conducted in support of traditional military operations, in particular the cyber operations conducted by some

[6] See Julia Kisielius, Breaking Down the SolarWinds Supply Chain Attack, SpyCloud, 11 March 2021, https://spycloud.com/solarwinds-attack-breakdown/.

Western states against the command and control centre of the Islamic State group alongside efforts to disrupt their propaganda strategy.[7]

Cyber operations in support of traditional military operations may also target weapons systems in order to make them inoperable. Although such operations may be difficult to carry out successfully, weapons systems that are old and therefore prone to security vulnerabilities in the control systems may pose attractive targets for adversaries.[8] As mentioned earlier (see section 2.1), cyber operations aimed at encrypting the adversary's data may also be among the methods used. Another noteworthy aspect of modern warfare in this context is the possibility of disrupting military satellite communication via cyber operations. In particular, the combination of cyber operations against ground stations or terrestrial communication links with kinetic attacks against satellites would be particularly disruptive, and may provide the attacking party with a significant military advantage, for instance if it were to disrupt GPS signals. However, such a far-reaching operation disrupting satellite communication would almost certainly severely affect the civilian population as well as third parties not involved in the conflict at hand.

Two further points are important in this context beyond questions pertaining to the particular operations. An expert noted that, in order to have the intended effect on the adversary, sophisticated military cyber operations will frequently require extensive intelligence gathering in peacetime before the beginning of an armed conflict. For this reason, decision-makers consider it essential to gain a foothold in adversary systems so as to be prepared for the conduct of military cyber operations when desired, a practice that has been called "preparing the battlefield" in cyberspace.[9]

Cyber operations in support of traditional military operations are also subject to the same planning considerations as traditional military operations. The transformation and modernisation of militaries in general but also regarding cyber capabilities in support of traditional military operations imply that the military will be more reliant on civilian infrastructure and services, for example for supply chains and critical infrastructure. Furthermore, the increased speed of operations might leave less time for reconnaissance and manoeuvring which could mean there is less time to take precautions to verify that the objectives to be attacked qualify as military objectives and that it is not prohibited by IHL to attack them.[10]

Furthermore, cyber operations in support of military operations are often chosen according to how effective they are to achieve a certain military aim. For example, where the target is to bring down an enemy military aircraft, such military aim is difficult to achieve by cyber operations directly. However, cyber operations can be efficiently used to target air traffic control or by controlling a drone instead. When using cyber operations in support of military operations, it is thus a common step to look for soft targets first. Unfortunately, this means that civilian targets are often considered to be the path of least resistance, which entails a further increase of societal risks and potential

[7] See Deborah Haynes, Into the Grey Zone: The 'offensive cyber' used to confuse Islamic State militants and prevent drone attacks, 8 February 2021, https://news.sky.com/story/into-the-grey-zone-the-offensive-cyber-used-to-confuse-islamic-state-militants-and-prevent-drone-attacks-12211740 (interview with two top-level U.K. officials). Further examples of states who have acknowledged using cyber operations during armed conflicts include the U.S. (https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf) and France (https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de-reussite-n-est-pas-le-nombre-de-djihadistes-tues_5488379_3210.html).

[8] See Lukasz Olejnik, The Dire Possibility of Cyberattacks on Weapons Systems, Wired, 10 March 2021, https://www.wired.com/story/dire-possibility-cyberattacks-weapons-systems/.

[9] See Karl Grindal and Karim Farhat, Persistent Engagement or Preparing the Battlefield?, Internet Governance Project, 24 June 2019, https://www.internetgovernance.org/2019/06/24/persistent-engagement-or-preparing-the-battlefield/.

[10] See (Art 57/2/a/i API), considered to reflect Customary International Law (Rule 16 CIHL Study). See generally ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts (Ewan Lawson and Kubo Mačák eds.), ICRC, Geneva, 2021.

humanitarian impact of cyber operations during armed conflict. From a state's perspective, however, relying on cyber operations as opposed to boots on the ground might mean that the state continues to enjoy more support for its war effort from its own population as it puts fewer human lives at risk directly.

Overall, cyber operations in times of conflict do not differ significantly from those during peacetime and in principle, the same methods and means are used. Both in times of peace and conflict, cyber operations have the general purposes of intelligence gathering and disruption. Differences do occur with respect to the targets selected but difficulties are expected when it comes to differentiating between civilian and military objects, as by default, cyber infrastructure contains a significant number of dual-use objects. In light of this fact, some experts contended that cyber operations conducted during armed conflicts might lead to more severe consequences for civilian populations than peacetime conduct, as the nature of conflict may incentivise military decision-makers to proceed with less caution in regard to civilian infrastructure and assets, leading to operations with more arbitrary outcomes. As seen in the case of Ukraine, for example, a conflict party's electrical grid may be targeted without due regard to the essential civilian functions that depend on the provision of electricity.

2.5. INTELLIGENCE GATHERING AND ESPIONAGE

Intelligence gathering is a crucial preparatory step for cyber operations. For example, it is often conducted to enable an information operation but also to "prepare the battlefield", as the effective execution of large-scale or otherwise sophisticated military cyber operations will regularly require extensive or even near-constant preparatory intelligence gathering, for example to detect weaknesses and vulnerabilities in adversarial systems and to parse out opportunities for adversarial conduct, including during times of crises such as a global pandemic. Furthermore, intelligence gathering is needed to make cyber operations more precise, not least in order to avoid harm to civilians or civilian infrastructure. At the same time, the amount of (private) data collected by means of intelligence gathering raises human rights concerns relating to privacy and data protection rights. Finally, it is worth pointing out that cyber operations to prepare the battlefield usually constitute of more than mere intelligence gathering, as they often involve planting malware in adversarial systems that later can be activated ("weaponised") if so desired.

Generally speaking, intelligence gathering as described above is a sub-category of traditional espionage. Whereas espionage itself is generally not considered illegal under international law, the question arises whether espionage in the context of military cyber operations should be classified differently from a legal perspective, in particular if it aims at preparing the battlefield. From a technical perspective, it is also to be considered more than mere intelligence gathering or "just espionage", as it may also have inadvertent paralysing effects on the system, even when no other activities such as outside data theft occur. In response, the victim network operators need to allocate resources and time to investigate the incident which could lead to systems downtime. Furthermore, the scale of data retrieved also differs significantly from traditional espionage and raises questions as to whether this changes the assessment of legality.

IV. OBJECTIVES

Cyber operations can be launched to fulfil a range of aims. Whereas for cyber criminals, the pre-dominant motivation might be of a financial nature, other cyber operations have different purposes that thus implicate other objectives. Of particular concern are those operations that are directed against society as a whole (section 3.1) or against trust (section 3.2). Generally speaking, in recent years there has been an observable trend among cyber powers to target processes essential for the functioning of the society rather than more limited objects (such as the industrial control system of a single target facility to cause physical effects).[11] Operations might be easier to identify when they are of a physical nature (see section 3.3) or when they target data (section 3.4). Especially the first two types of operations bear significant risks and consequences which are harder to grasp and measure.

3.1. OPERATIONS AGAINST SOCIETY

Cyber operations that are of particular concern are those operations that are directed against society as a whole and have the objective of destabilising it, for example by interfering with or disrupting essential societal processes such as voting, taxation, or education. Methods to achieve such wide-ranging and far-reaching impacts on the entire societies can be achieved, for example, by conducting offensive cyber operations against the infrastructure that provides crucial services or by carrying out complex information operations that aim at undermining trust in public institutions (see also section 3.2 below). At the same time, the experts voiced doubts as to the likelihood of a military cyber operation having sustained, large-scale societal effects to the extent of "bringing down" an entire society by way of cyber force. Such impact is difficult to achieve at least over a longer period of time, especially as people are capable of adapting to crises. The coordinated execution of various cyber operations would be necessary to achieve such aim, which seems to be a less imminent threat in the near term.

In this context, the cyber operations in Ukraine in 2014 were discussed as an example of how cyber operations could affect an entire society. Here, cyber operations to paralyse the network infrastructure in Ukraine were coordinated successfully just shortly before tanks crossed the border. Cyber operations are therefore becoming a clear component of other military operations and the Ukraine example shows how a network-based attack to shut down the internet in a given region has already been used as a strategy. Even though it should be emphasised that the Ukraine example also shows that such far-reaching systemic effects on society will often only last for a short period, it was noted as significant that the offensive operations *inter alia* affected the computer systems that pharmacies in Ukraine use to locate medication, potentially making it more difficult to civilians to get a hold of their medication. Such an outcome at the very least hints at the potential gravity of this type of cyber operation that targets essential societal functions like network infrastructure.

As mentioned, of particular concern were those information operations designed to achieve large-scale societal effects, in particular those with the purpose to cause the erosion of the trust and social cohesion that are necessary for modern open societies to function. Such negative outcomes may be triggered, for example, by targeting essential societal processes such as elections or the workings of financial institutions or the economy at large. Even if any long-term impact remains unlikely, the cyber tools facilitate the attempt at achieving such ends. Whereas in the past, adversaries had to make a choice between having a wide impact for a short duration or a deeper impact but for a more narrowly defined target group, such choice is now no longer needed. Instead, the increased interconnectivity of society but also the use of insecure internet-of-things devices or industrial control systems at least potentially allow attackers to increase negative systemic consequences on target societies. Operations that aim at affecting societal trust in particular will be elaborated on in the next section.

Overall, large-scale operations that would lastingly destabilise an entire society are very difficult to conduct. However, such sophisticated, large-scale operations are not necessarily needed to achieve a certain goal, as even repeated small-scale disruptions or

[11] See in more detail Robin Geiss and Henning Lahmann, Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats, Geneva Academy Working Paper Series, February 2021, https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf.

operations of less sophistication can affect the society as a whole.

3.2. OPERATIONS AGAINST TRUST

Cyber operations with the purpose to erode a civilian population's trust in a state's political system and in its institutions are especially concerning. For one, such outcomes may be achieved by way of concerted disinformation campaigns or other types of information operations, in particular if supported by the employment of artificial intelligence. While large-scale operations can reach a considerable level of complexity that make them very resource-intensive, corrosive effects on societal cohesion can already be achieved with comparably cheap means. For example, if existing social media platforms are utilised to spread disinformation, aiming to impact the minds and psychological capacities of the target population, information operations can become very extensive without requiring large resources.

For instance, information campaigns may spread distrust among target demographics regarding the functioning of financial institutions and the financial system at large, potentially causing a large number of individuals to withdraw their assets from banks. This shows that it is not absolutely necessary to target the bank directly but that the same effect can be reached by deploying a disinformation campaign that might even be relatively cheap if compared to a sophisticated cyber operation against the financial institution's typically well-protected IT systems, relying instead on achieving indirect effects by manipulating the behaviour of individuals. Elections, considered a soft spot in society and a target that would allow an adversary to bring about change in a society with relatively low effort, are particularly vulnerable. Aside from possible economic and financial harm or political change, these potential instabilities can also cause large-scale loss of societal trust causing existential risks to societies in the long run. In the most extreme cases, such a development could even lead to civil unrest or riots.

A particularly pressing problem in this context is the fact that loss in trust is difficult to assess and measure. Whereas some aspects can be examined over time, for example by evaluating voting behaviour, such developments are more mid- to long-term and the analysis thereof takes time. The assessment of an erosion of trust thus does not operate at the same speed required to effectively respond to such information operations. Furthermore, this task is complicated by the fact that causation is also hard to prove in this context.

Overall, the loss of integrity of certain institutions could potentially have a bigger impact than certain kinetic effects might achieve. Most of the time, physical objects or infrastructure can be repaired. Re-establishing trust, on the other hand, is an extremely difficult and time-consuming task, assuming that is possible to do so at all.

3.3. OPERATIONS CAUSING PHYSICAL HARM

Generally, there have been fewer cyber operations with physical effects than many observers had expected a decade or two ago. The main reason for this is that such operations are highly complex and physical assets make for difficult targets. States may also be reluctant to conduct operations that have physical effects as these would probably rely on their most potent cyber capabilities, which the states are reluctant to reveal unless it is in order to achieve a considerable strategic gain. As long as it is feasible, it is more likely that states resort to operations that require less effort and fewer resources first. Relatedly, where the same or a similar aim can be achieved by other, non-cyber means, such means may be preferred given the complexity of cyber operations required to achieve it.

At the same time, this does not mean that there is no risk at all of future cyber operations causing physical damage. Although not many operations against physical objects have been carried out to date, they are nonetheless well within the realm of possibility, especially in light of the proliferation of capabilities and tools. Actors that are less skilled in these areas but have the necessary budget could purchase offensive cyber tools, such as exploits or malware, or services on the black market in order to carry out operations that cause physical harm on a large scale. Although such conduct was not considered particularly likely, some experts noted that its possibility should not be dismissed.

Hypothetical examples of operations against physical objects include operations to bring down a plane or operations directed against military equipment such as weapons systems (see section 2.4 above). Attacks against global communication systems such as satellite links or navigation systems could also have especially devastating effects.

Further concern was raised with respect to operations against core internet services and infrastructure. One expert argued that whereas operations deployed to merely affect assets consisting of bytes and bits or of silicon – all relatively easy to rebuild – more sophisticated operations, for instance those that target industrial control systems, are inherently considerably more harmful. Such systems are essential to safely run many types of critical infrastructure such as electrical grids, and their failure may easily lead to physical damage, impairing the targeted infrastructure in a way that makes quick restoration difficult. As a result, entire cities may be cut off from basic resources like electricity or clean drinking water, which would cause significant suffering amongst the affected population.[12]

Critical infrastructure in particular may present itself as a potential target for cyber operations in the future (see also section 4.3 below). In this context, the experts discussed the hypothetical example of an offensive cyber operation targeting traffic lights or train control systems with the potential consequence of accidents, leading to physical harm. However, one expert demurred, arguing that affecting a train control system in this manner would likely merely lead to a disruption of service. In light of existing safety systems in such large-scale infrastructure, any effects would be limited to affecting the train schedule – certainly an inconvenience, but far off from threatening the physical integrity of the assets or even humans.

This example, however, points to another important aspect: the question of what should be considered physical harm. The lack of a tangible threat to life and limb in such scenarios notwithstanding, possible long-term effects that may even lead to decreased life expectancy when certain essential services are disrupted should not be neglected when assessing potential harms.

3.4. OPERATIONS AGAINST DATA

Large-scale effects could also occur when cyber operations target personal or non-personal data. This might involve, for example, medical records but also other data such as tax records or social security data. In this respect, manipulation of data may be more damaging than mere access or perhaps even than the deletion of data, as the alteration of data might obscure what data was manipulated and to what extent. Such uncertainty can further spread distrust among citizens, in particular towards the institutions managing these datasets, for example tax authorities. While data records are frequently accessed for espionage purposes, they are usually not erased systematically, as such a step would be seen as a further escalation.

Some experts raised particular concern with respect to large-scale data leaks, a trend that will likely further increase in frequency. Such data can encompass digital ID profiles including biometric data and also medical records, as was recently the case with a large-scale data leak in Brazil, which reportedly exposed the medical records of 243 million citizens.[13] Such leaks are considered especially worrying given that they include data that is not subject to change (biometric data as opposed to passwords) and further puts the victims of such incidents at risk of becoming victim of further acts of cybercrime in the case

[12] See in detail Sergio Caltagirone, Industrial Cyber Attacks: A Humanitarian Crisis in the Making, ICRC Humanitarian Law & Policy, 3 December 2019, https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/.

[13] https://www.cpomagazine.com/cyber-security/brazils-health-ministrys-website-data-leak-exposed-243-million-medical-records-for-more-than-6-months/

that criminals obtain the leaked sensitive data, for example by way of subsequent blackmailing.

V. VULNERABILITIES

The same type of cyber conduct can have different consequences depending on which individuals, societies, or even sectors are targeted. The impact largely depends on how susceptible the respective target is to the effects of the cyber operation. Based on this premise, the experts discussed the factors that make some individuals particularly vulnerable to adversarial cyber operations but also which public or private sectors might suffer particularly grave consequences when targeted. Of particular relevance in this section were the discussions surrounding critical infrastructure but also the vulnerabilities of the society at large. The different groups will be addressed in turn.

4.1. INDIVIDUALS

Depending on the interests at stake, it is less likely that individuals will be attacked directly, at least as far as military or otherwise state-led cyber operations are concerned. Individuals can be considered both the weakest and the strongest link in cyber security. Whereas there are plenty of examples of individuals not observing an adequate level of "cyber hygiene", for example by failing to install critical security updates to keep their systems up to date, on other occasions, individuals might also be able to detect suspicious behaviour, for example when monitoring activities of others accessing the same network.

4.2. PRIVATE SECTOR

As previously mentioned, the private sector is particularly vulnerable to ransomware attacks, especially where outdated software is used, or the adequate level of "cyber hygiene" is not observed in regard to a company's IT systems. This general problem concerns virtually all medium-sized companies, but some sectors are particularly vulnerable to adversarial cyber operations given their low cyber maturity level. As mentioned, this relates especially to the health care sector, which has in many countries been underfunded with respect to cyber security. In contrast, the financial sector has commonly allocated a bigger budget to cyber security measures and although subject to frequent attacks, has achieved a considerably higher cyber maturity level. Other sectors that have been highlighted as particularly vulnerable are pharmaceutical and manufacturing companies where production sites often operate with old equipment. While these outdated tools and machines are expensive to replace and will thus remain in operation long after security updates for their operating or control systems have been developed, their vulnerabilities are often well-known to potential adversarial parties. Even where manufacturing sites operate with an internal network that is "air-gapped", i.e. not connected to the internet, they remain vulnerable to hacks, especially when insider information is passed on or an intruder is able to enter the manufacturing site in person.

Vulnerabilities can also be found in those sectors that have quickly digitalised or introduced new technologies rapidly without spending adequate resources to put in place state-of-the-art cyber security systems and policies that are able to protect their assets, such as firewalls or intrusion-detection software. In such cases, security weaknesses have to be addressed retroactively, which increases the likelihood of undetected vulnerabilities.

Furthermore, increased vulnerability also stems from risks in supply chains. Often, software vendors are unaware of third-party code in their products. Consequently, there is no awareness or understanding of possible vulnerabilities which in turn cannot be addressed adequately. This is highly relevant for manufacturing processes, where a company might supply a system that relies on other, smaller components that might be compromised. This is a particular issue when it comes to internet-of-things devices that are often produced as cheaply as possible, which implies that manufacturers use software that is quickly outdated and cannot be updated – as this would require provisions that would increase cost – leaving the devices exposed to hackers.

Finally, many companies or facilities lack qualified employees to implement cybersecurity measures. This might be because their specific institution is underfunded, as is the case in particular in the water and healthcare sectors in many states. Many small and medium-sized companies also lack a sufficient budget to hire staff qualified in cybersecurity. Moreover, many vacancies remain unfilled given the lack of qualified and experienced cyber security experts.

4.3. PUBLIC SECTOR AND CRITICAL INFRASTRUCTURE

An increase in vulnerability can also be seen with respect to critical infrastructure, an area in which there has been an increased commoditisation of attacks. Due to large-scale privatisation, particularly in Western countries, many critical infrastructure providers are no longer part of the public sector. Increased vulnerability partly stems from the confluence of operational technology (OT) and information technology (IT) networks, for example when industrial control systems (ICS) are connected to IT for remote maintenance purposes. Attacks against industrial control systems and industrial environments are growing at a considerable pace.

Again, increased interconnectedness is a crucial factor with regard to many different types of critical infrastructure, for example where medical equipment is connected to the internet; water supply systems are also increasingly digitalised. Critical infrastructure systems are particularly vulnerable – potentially even to nation-wide effects – where they rely on the same operating or industrial control software across sectors and providers (see supply chain risks, section 2.3 above). The latest versions of sophisticated malware, including ransomware, are capable of detecting automatically the type of ICS they have breached, i.e. these types of software are “aware” whether they are inside systems that control, for instance, a water main or an electrical grid. This allows for higher precision in targeting and at the same time increases the vulnerability of critical infrastructure in terms of falling victim to “Big Game Hunting” (see section 2.1 above).

Throughout the discussion, it was stressed that the protection of critical infrastructure is a topic that remains generally understudied and that the term itself is defined differently in each country or region. Regional particularities matter a great deal for the question of what qualifies at “critical”. In this context, one expert remarked that in certain sub-Saharan African countries , due to a general lack of terrestrial network infrastructure, mobile communications are much more critical than other IT systems for the purpose of essential societal services such as micro-finance, healthcare payments, or prepaid electricity. It was further pointed out that the vulnerabilities of certain sectors may diverge depending on the country or region. Whereas the financial sector is by and large well secured against adversarial cyber operations in Western countries, the same cannot be said for certain countries in the Global South that have less developed cyber security standards.

The question of what constitutes critical infrastructure has important implications as its protection might vary accordingly. Furthermore, whether a sector is considered a critical infrastructure as well as the extent to which a particular sector is at risk also varies over time and depends on the interests of the attacker in a given case. A particular sector might also be particularly valuable at a point in time due to external factors and therefore especially vulnerable to malicious cyber conduct.

Recent trends, some having to do with the COVID-19 pandemic, have confirmed that the health sector is particularly vulnerable, especially given the limited budget it typically allocates for cybersecurity. Further vulnerability stems from the expectation that those responsible for healthcare facilities are expected to quickly pay up ransom when subject to ransomware attacks given there potentially are lives at stake. A special case is the increasingly common practice of connecting critical medical devices like pacemakers or ventilators to the internet for the purpose of remote maintenance adds a further layer of increased vulnerability that puts both the healthcare providers and the directly affected individual patient at a high risk of harm. Several experts explicitly raised the concern that operations against hospitals may result in the deaths of patients at some point in the future.

Further vulnerability is often found with respect to water facilities which some experts considered the biggest issue in critical infrastructure protection. Unlike electricity infrastructure, water providers are generally "hyper local" and decentralised. Due to small budgets, water infrastructure is typically one of the least secure industries.

There are many individual water utilities, each supporting a relatively small number of households, meaning that where these are attacked, only a relatively low number of households are affected unless situated in metropoles like New York City or Tokyo. Here, the water infrastructure usually resembles that of electricity grids, meaning that they are run by a consortium of water utilities. Consequently, an adversarial cyber operation against a single provider could potentially have negative effects on a larger population. Moreover, different infrastructure systems are also interdependent. With respect to water supply systems this means that when there is no electricity, most water pumps also stop working, which further increases vulnerability. The same holds true for most other types of critical infrastructure, even if some of them – most importantly healthcare facilities – are often obligated by law to have backup power supply systems available in the case of an emergency situation such as an ongoing cyber operation against the electrical grid.

Even in the case that a cyber operation affects the quality of drinking water only to a limited extent without in fact rendering it detrimental to human health, just the appearance of tampering can already have a negative psychological impact on the civilian population, for example when uncertainty about the consequences of a cyber operation against a water facility prompts authorities to order citizens to boil all water before consumption. Furthermore, the provision of water is vulnerable to service breakdowns as it is not easily transportable. In such a crisis, it could quickly become difficult to provide clean water to the population, in particular to remote areas.

Another noteworthy area in this context is the transportation and logistics sector. Over the course of the digital transformation, for example, many warehouses have been transformed into "smart warehouses" that heavily rely on IT systems and functioning network infrastructure, whereas cyber security standards have not always kept pace with this rapid development. The same increasingly holds true for entire major ports. Adversarial cyber operations against such facilities of the transportation sector, for example by way of ransomware attacks that encrypt logistical data or affect digital navigation systems, can have serious ripple effects if they affect the functioning of supply chains of critical goods like medication or healthcare devices.

One expert underscored that sectors that have not yet been attacked may be more vulnerable than those that have already had to deal with numerous cyber incidents. This is because cybersecurity incidents experienced by a company or by other companies in the same sector generally increase awareness and generate willingness to spend more resources on addressing vulnerabilities and further fostering cyber resilience.

Dependencies on single infrastructure systems or single providers can further increase vulnerabilities. One example is a country which overwhelmingly relies on only a single seaport, e.g. for the trade of medical supplies. In less developed countries there is far less diversification in electricity and water supply utilities resulting in many people being dependent on single sources of supply, thus rendering a society particularly vulnerable.

However, the increasing number of observed cyber operations against critical infrastructure such as water systems has to be assessed with caution. Given the increased attention on the matter, there is a certain visibility bias. In addition, the increased interconnectivity has made the networks more vulnerable and attacks more successful, yet that does not mean they did not exist before water systems received more attention.

4.4. SOCIETY

The vulnerability of a society largely depends on its level of technology integration, as higher interconnectivity implies the potential that cyber operations have a more severe impact, a trend that is amplified by society's demand for increased digital functionality. The impact of adversarial cyber operations is directly proportional to how much societal processes and human lives are digitally integrated and the degree of reliance on digital, interconnected technologies. This can vary depending on a society's demographics; factors such as age generally determine dependence on technology. At the same time, one expert considered both the youngest and the oldest members of society as the most vulnerable given the limited cyber security awareness among these age groups, which makes them easy targets for phishing attempts or scams related to online banking.

The impact cyber operations have on society furthermore depends on the timespan for which they last and whether they are combined with other measures. A short power outage might have less of an effect than a longer period without electricity; moreover, a society that is more used to power cuts will be less vulnerable to such an attack than others. In addition, a society might be especially at risk if there is an Internet shutdown and propaganda is spread via text messages. Not simply an especially cheap tool for communication, this method of dissemination of information also significantly decreases citizens' ability to independently fact-check the validity of such information via online resources. Such a situation might thus further exacerbate distrust in government and institutions.

Generally speaking, civilian entities and processes represent a softer target for military cyber operations than adversarial armed forces. As mentioned, electoral processes are particularly soft and vulnerable targets and attractive to those who want to foment conflict or manipulate the political landscape and situation of a country. In this respect, some experts pointed out that less developed countries might be more susceptible to such attempts due to generally more fragile and less developed democratic systems. Information operations targeting elections will exacerbate mistrust and scepticism towards the democratic process. Propaganda and disinformation could also cause communal tensions, and in worst cases even lead to election-related violence.

This example shows that it is crucial to emphasise that the fact that societies are particularly vulnerable where interconnectivity is advanced does not only apply to Western countries, but also to the Global South, where dependence on certain technologies such as text messaging or single social media platforms that act as de-facto monopolies can be particularly pronounced. Such a situation may create single points of failure or other systemic risks.[14] One prominent example in this context is the spread of disinformation and hate speech on Facebook in Myanmar.[15] Another example brought up by the experts was Ethiopia, where, despite relatively limited technological integration among the society, misinformation, disinformation, and hate speech have exacerbated tensions and led to acts of violence on the ground.[16]

Aside from interconnectivity, there are other noteworthy external factors that can further contribute to a society's vulnerability. One expert suggested that the further away the target of a cyber operation is from conflict and poverty, the more likely it is – at least as it currently stands – to only cause disruptive

[14] See also ICRC, *Harmful information: Misinformation, disinformation and hate speech in armed conflict and other situations of violence*, ICRC, 2021, https://www.icrc.org/en/publication/4556-harmful-information-misinformation-disinformation-and-hate-speech-armed-conflict.

[15] See Paul Mozur, A Genocide Incited on Facebook, with Posts from Myanmar's Military, New York Times, 15 October 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[16] See Peter Mwai, Ethiopia's Tigray Conflict Sparks Spread of Misinformation, BBC, 11 November 2020, https://www.bbc.com/news/world-africa-54888234.

harm. In contrast, a cyber operation that for example targets the organisation of humanitarian aid efforts by disrupting communication systems could be more likely to cause physical harm.

SPOTLIGHT CASE STUDY: COVID-19

The Covid-19 pandemic may serve as a paradigmatic illustration of how a range of factors that are not directly related to cyber security issues in combination with a change in context can influence and impact societal risks and vulnerabilities vis-à-vis adversarial cyber activities.

Firstly, the advancing digitalisation in general but also the sharp increase in remote working in particular have exposed users and companies to new threats. Most significantly, the practice of logging into company networks remotely by employees working from home renders companies more vulnerable, as many lack sufficiently advanced security protocols for their cloud-based services. Other potential targets are home routers due to their frequently insufficient cybersecurity standards, even though so far experts have not observed an increase in attacks against them. Furthermore, individuals have been targeted by means of Covid-19-themed phishing campaigns and disinformation. Individuals have also been subject to ransomware attacks, with attackers reusing existing malware but adapting it to Covid-19 themes.

Secondly, the Covid-19 pandemic has further exposed how vulnerable the health care sector is. Even before the beginning of the pandemic, hospitals and other health-care facilities proved susceptible to adversarial cyber conduct due to a traditionally low cybersecurity budget and thus a low overall cybersecurity maturity level (see section 4.3 above) in comparison with other sectors such as finance. Placed under severe pressure because of the pandemic, hospitals became especially vulnerable to cyber operations, e.g. ransomware attacks. A much-discussed incident occurred at the University Hospital Düsseldorf in September 2020. While a ransomware attack had incapacitated the hospital's computer systems, a patient in critical condition could not be admitted to the emergency room and then died on the way to another hospital. Although a later investigation rejected the hypothesis that the cybersecurity incident had in fact caused the patient's death, experts underscored that this may well happen in the near future.

Thirdly, since the start of the pandemic, there has been an increase in disinformation campaigns related to Covid-19 in general and those targeting trust in vaccines in particular. For example, the false information that 5G technology spreads the virus was shared widely. Information operations like these are particularly difficult to counter as they are amplified on social media but also given the limited research and a lack of scientific consensus at least in the early stages of the pandemic, e.g. with respect to the origin of the virus, possible remedies, or the effectiveness of public health measures.[17]

Aside from vaccine disinformation, there have also been cyber operations directly targeting vaccine research and public vaccination efforts, e.g. in the form of "vaccine espionage" against research facilities and other institutions working on the development of vaccines, but also other cyber operations such as ransomware attacks against companies conducting medical research.[18]

[17] See US Gov: https://www.cisa.gov/publication/covid-19-disinformation-activity.

[18] See M. Schmitt, 'Cyber Operations against Vaccine R & D: Key International Law Prohibitions and Obligations', *EJIL:Talk!*, 10 Augist 2020, https://www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/.

VI. RESILIENCE

The impact of cyber operations not only depends on the target's vulnerabilities, as addressed in the previous section, but also directly relates to questions of resilience, such as "How prepared is the target to prevent a cyber operation against its systems?", or "Does a company that has become a victim of a ransomware attack have backups of their data and can thus recover quickly?" To improve resilience, various steps can be taken to prevent cyber harm, for example, advanced cyber hygiene measures or improving wider awareness of security weaknesses. In situations in which societies are targeted by information operations, long-term educational measures are needed to make societies more resilient to disinformation. Other key topics include attribution, in relation to which experts disagreed on its deterring impact, as well as recovery, a topic that several experts felt was often not addressed sufficiently.

5.1. PREVENTION

SAFETY AND SECURITY MEASURES

In order to prevent vulnerabilities, two decisive steps can be identified: (1) adequate recognition of an existing problem, and (2) appropriate investments to address it. The need for preventive measures is further increased in light of the observation that generally speaking, defensive capabilities are mostly years behind the development of offensive capabilities. Prevention of cyber operations can be strengthened by certain state-of-the-art technologies, e.g. AI-driven intrusion detection. However, the problem remains that most sophisticated defensive measures require adequately trained staff in order to employ such tools correctly, a crucial aspect that (potentially) affected companies or institution still often lack. Even the best tools are ineffective in the prevention of cybersecurity incidents if implemented by inexperienced or ill-trained employees.

With respect to ransomware attacks, prevention can often limit the impact of the attack, e.g. by employing state-of-the-art software to detect the operation during the exploitation phase, which might facilitate the disruption of this process. Moreover, it is possible to interrupt the encryption process by deploying tools that can generically detect that encryption is ongoing and will prevent the conversion of the original data into something else.

With regard to the prevention of supply chain risks, it was suggested that manufacturers should provide their customers, users, and developer ecosystem with more information and tools that would enable them to understand current and future threats in order to better protect themselves. Suppliers should also protect their customers and users by designing, developing, and delivering products and services that prioritise security, privacy, integrity, and reliability. This would in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities and could significantly contribute to the prevention of supply chain attacks.

Other longer-term measures to increase security levels that should be considered include observing a well thought out cyber hygiene, a sensible measure that is premised on having acquired general awareness of cyber security issues as a first step. For one, this entails avoiding the use of outdated software to eschew so-called legacy problems. Importantly, the actual implementation of policies is or course essential to increase the level of cybersecurity. In this regard, some experts criticised that the focus too often lies with developing elaborate cyber security policies, without however paying adequate attention to the crucial subsequent step of effectively implementing them.

An important step towards increasing the overall cyber security level is enhanced cooperation between public institutions and private sector companies, for instance to share cyber security information. In this regard, any effective cyber threat intelligence analysis should happen on a global level and always take into account the perspectives from both the public and the private sector. Only if all sectors work together and inform one another of threats observed in their systems, other actors can prepare their defences more accurately and thus improve their resilience to further attacks. However, such cooperation requires mutual trust between the actors. While some countries, such as Switzerland, have made good progress in this regard, others still lag behind. One expert even suggested the implementation of an international cyber defence mechanism to prevent malicious attacks against critical infrastructure on a global level.

In the context of critical infrastructure protection and resilience, one expert highlighted the crucial distinction between “security” and “safety”. Even if the cyber security level of critical infrastructure providers is not always up to the task, meaning that it may be possible for malicious parties to launch adversarial cyber operations against them successfully, that does not necessarily imply that physical assets or even individuals are endangered. Generally speaking, existing safety protocols in most critical facilities (such as water-processing units) require employees to monitor their correct functioning (such as drinking water quality) without exclusively relying on IT systems. This extra layer of safety that operates independently of cyber security measures is highly relevant for questions of resilience and the managing of cyber threats.

RESILIENCE AGAINST DISINFORMATION VULNERABILITY

One frequently highlighted strategy to decrease a population’s vulnerability to disinformation is the stepping up of efforts to teach digital literacy. Positive results in this regard have already been observed in several Baltic and Nordic countries. Here, pupils are taught to critically approach new information, to question the sources and to scrutinise the quality of information.[19] More generally, the detection and identification of both false or misleading content and deceptive disseminators of disinformation are particularly crucial. Some of the experts additionally stressed the critical importance of building counternarratives to fend off the effects of concerted adversarial disinformation campaigns.

SOCIETAL PREPAREDNESS

It is important to underscore the societal preparedness for situations of serious cyber security incidents. This can be increased by educating the public on what to do in case of large-scale impacts caused by cyber operations, for example if all communications infrastructure breaks down. This could be similar to, for instance, public exercises in order to prepare for an earthquake. An example of a nationwide strategy to adequately prepare the whole of society can be found in Sweden. Here, a pamphlet was delivered to all residents by the Swedish government, stating that in case of the need to counteract cyber effects causing a complete digital shutdown, all communications would be redirected to radio, pointing to car stereos in the event of a loss of power.[20] However, the same model may not be equally effective in countries with a larger population or in societies with a lower degree of social cohesion.

5.2. ATTRIBUTION

Although capabilities to attribute adversarial cyber operations have generally improved over the past decade, attribution of cyber operations very often remains a difficult and time-consuming task. However, attribution is crucial for a number of reasons. For one, by removing plausible deniability, it can have a deterring effect on would-be attackers. Furthermore, the process of attribution often reveals important facts about the means and methods of adversarial cyber operations, which can subsequently be utilised to develop future technical defence mechanisms. Nonetheless, it has also become evident that attribution is not necessarily a

[19] See e.g. Maarit Jaakkola, Media literacy in the Baltics: Different approaches in neighbouring countries, *Media & Learning*, December 2020, https://media-and-learning.eu/type/featured-articles/media-literacy-in-the-baltics-similar-backgrounds-but-different-approaches/.

[20] Swedish Civil Contingencies Agency, If Crisis or War Comes, May 2018, https://www.documentcloud.org/documents/4481608-Om-Krisen-Eller-Kriget-Kommer-Engelska.html#document/p1.

primary goal of every targeted actor.

Some experts stressed that attribution itself is not always necessary for good cyber security practices at least when it comes to the industrial sector, as patching in a timely manner is more crucial but does not require attribution. It is, of course, more relevant for political purposes and in order to take other retributive steps such as the imposition of sanctions.

Attribution is made more difficult by actors trying to cover their tracks by launching false-flag operations. It is a complex task to determine whether a third party is pretending to be a different entity, e.g. another state, or whether the operation actually originates with the suspected actor or state. This is a problem particularly with respect to malware attacks, as the malicious software itself is often the only piece of forensic evidence left behind by the attackers. Given the trend towards false-flag operations, attribution based solely on the code itself can often not be made with confidence. Instead, political motives and strategic incentives have to be taken into account in addition to forensic evidence.

Whether attribution actually serves purposes of deterrence was subject to debate among the experts. Some argued that it principally depends on the actor in question. Whereas individuals might face legal consequences and thus might be deterred by the prospect of being identified in the aftermath of a cyber operation, it is questionable whether the same consideration applies to nation states that are frequently able to maintain a degree of plausible deniability even in the case of strong evidence against them. However, some experts suggested that more frequent and public attribution of malicious cyber operations might ultimately lead to a deterrent effect.

Other experts were generally more optimistic, stressing that law enforcement makes progress in attributing cyber operations and holding individuals responsible. One example mentioned in this context was Operation Ladybird, a combined effort of several police forces to take down malware called “Emotet” which had grown into a large number of botnets that targeted victims with ransomware and data theft.[21] As such, cyber criminals are increasingly aware of the risk they are taking, which is reflected by the increase of operational security measures taken by criminal actors in order to protect their systems against discovery.

Finally, a general challenge with respect to attribution relates to the credibility of attribution statements, which depends to a large extent on the actor making such a claim. To make allegations of malicious cyber conduct more convincing in the eyes of the public, one expert suggested the establishment of a neutral, internationalised fact-finding mechanism to clarify the attribution of cyber operations and to attribute malicious behaviour to those responsible. However, it was acknowledged that such a mechanism would be challenging to establish in the current geopolitical situation.[22]

5.3. RECOVERY

The impact of an operation significantly increases when reaction and recovery are slow. This is especially true concerning incidents that target a population’s trust in governmental institutions, but also regarding small and medium-sized businesses which often have difficulties to recover from cybersecurity incidents. When a company falls victim to a ransomware attack, the question arises whether to pay the ransom in order to receive the key to decrypt its files. One problem is that there is no guarantee for such exchange to be successful. In addition, the hacker might be able to re-enter the system through the same breach and extort the company once again. Experts generally agreed that it is therefore usually not advisable to pay the ransom. Moreover, recently there have been lists of victims willing to pay circulating on the dark

[21] See Andy Greenberg, Cops Disrupt Emotet, the Internet’s ‘Most Dangerous Malware’, Wired, 27 January 2021, https://www.wired.com/story/emotet-botnet-takedown/.

[22] See also Yuval Shany and Michael N. Schmitt, An International Attribution Mechanism for Hostile Cyber Operations, *International Law Studies*, Vol. 96, 2020, pp. 196–222.

web, making a paying company susceptible to repeated ransomware attacks. A better alternative is for the victim not to pay the ransom and instead try to find the breach and close it in order to improve its cyber security and to subsequently rebuild its systems.

Victims of a rudimentary ransomware attack also have the chance to advance recovery by decrypting their data with the help of free decryption tools. Most importantly, regular back-ups of data are essential in order to speed up the recovery process by enabling access to the original data. Moreover, identifying and closing the vulnerability through which the attackers gained access to the company's systems remains crucial. Other steps to enhance recovery and prevent damage to the company's reputation and loss of confidence of consumers include a good PR response as well as legal action. In this regard, one expert suggested that transparency about the occurrence of a ransomware attack from the start might be beneficial to an affected company.

Given difficulties to recover from various attacks, the number of insurance products for cybercrime risks has increased significantly. In some instances, the insurance company might be the party paying the ransom. This was viewed critically by some of the experts, as such a practice might incentivise insured companies to become less diligent in regard to their cyber hygiene, knowing that the insurance will step in if a security incident occurs. Moreover, if the insurer pays up the ransom, an attacker might be encouraged to repeat the crime. However, this might not always the case: After the "NotPetya" cyber operation had crippled the IT systems of multiple major companies, their insurers refused to cover the losses on the grounds that the operation, which Western powers had attributed to Russia and which had allegedly occurred within the larger conflict between Russia and Ukraine,[23] was to be qualified as an "act of war", thus contractually precluding the obligation to pay.[24] The technical value of insurance was also assessed with caution, as some experts raised doubts as to whether insurance in fact improves cyber security. Instead, they argued that the belief to be protected might incentivise a company to take more risks. Similarly, cyber criminals may be motivated to target the insured companies, given that they are perceived as more likely to pay. However, when insurance products offer incentives for good cyber hygiene, e.g. with lower premiums, insurance could indeed be regarded as helpful.

VII. IMPLICATIONS FOR THE APPLICABLE LAW

The current, quickly shifting landscape of global cyber threats as described by the experts during the workshops has different implications for various legal fields. Some of these aspects were briefly addressed during the workshops. In lieu of an overarching conclusion of the expert consultations and to point to aspects that merit further engagement by legal scholars and political decision-makers, a few subject areas will be highlighted in this section.

First, with respect to the accelerated proliferation of offensive cyber tools, one may consider some kind of regulatory mechanism to control the dissemination and use by states of at least those types of malware with the most dangerous potential for individual civilians and civilian population. As a case in point, self-propagating malware that attacks civilian and military targets alike is by default indiscriminate and thus prohibited in times of armed conflict. However, the possibility of

[23] See e.g. United States, Statement from the Press Secretary, 15 February 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/; Australian Government Attribution of the "NotPetya" Cyber Incident to Russia, 16 February 2018, https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf.

[24] See e.g. Adam Satariano & Nicole Perlroth, Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong, New York Times, 15 April 2019, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

making a malicious code's ability to make such distinction mandatory found favour with the participants. Some underscored that it is technically feasible to write malware that even if self-propagating from system to system, it only executes its payload once it has entered a previously defined target. One expert noted that already the Stuxnet malware had been designed in such a highly precise and discriminatory manner, and thus although it infected thousands of IT systems in various countries, it only did damage to Iranian uranium enrichment facilities, as was reportedly intended.[25] Aside from the substantial issue of how to verify compliance, making such ability to precisely distinguish between targets mandatory – beyond the more limited context of the principle of distinction in international humanitarian law – should be considered by states that develop or obtain offensive cyber tools.

A second subject area concerns the topics of information operations and espionage. With regard to the former, whereas the experts were in agreement that the problem of adversarial conduct resorting to means of false or misleading information to target populations in other countries was growing rapidly, with potentially far-reaching and long-lasting negative impacts, there was general scepticism as to whether such activities could be adequately addressed by means of (international) law in view of the difficulty to define such conduct and assess and measure harm. Concerning espionage, the experts questioned whether the traditional paradigm that such practice is neither permitted nor prohibited by existing international law is satisfactory in light of the potential negative consequences caused by the pervasiveness of online surveillance or by intelligence practices that aim at "preparing the battlefield".

Finally, questions were raised as to the future role of non-military actors during cyber conflicts. As the core network infrastructure is mostly in the hands of private entities, such companies might be in a position, or even under a duty, to suppress malicious conduct, while there may also be an urgent obligation for parties to armed conflicts to avoid harm to such infrastructure in light of potential negative ramifications for the global networks that modern society depends on. A parallel trend noted during the consultations is the growing involvement of civilian intelligence agencies in military cyber operations. From the perspective of international humanitarian law, the engagement of civilian actors – both private or public – in tasks traditionally associated with State armed forces poses the question whether and when such conduct qualifies as direct participation in hostilities, and thus leads to the loss of protection on part of the individuals concerned.

[25] See P.W. Singer, Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons (2015) 47 Case Western Reserve Journal of International Law 79, 85.

ANNEX 1: LIST OF EXPERTS

INVITED EXPERTS

- Mr Benjamin Ang, Centre of Excellence for National Security, Nanyang Technological University, Singapore
- Mr Lior Bar-Lev, Independent cyber resilience expert, Israel
- Mr Bernhards Blumbergs, CERT.LV, Latvia
- Mr Sergio Caltagirone, Cyber Threat Intelligence, Dragos, United States
- Mr Jason Healey, Columbia University's School for International and Public Affairs, United States
- Mr Bart Hogeveen, International Cyber Policy Centre, Australian Strategic Policy Institute, Australia
- Mr Reto Inversini, Swiss Government Computer Emergency Response Team, Switzerland
- Mr Vitaly Kamluk, Kaspersky, Singapore
- Mr Max van Kralingen, IT Security & Risk Management, Merck & Co., United States
- Ms Marina Krotofil, ISSP - Information Systems Security Partners, United Kingdom
- Ms Tang Lan, China Institutes of Contemporary International Relations, China
- Mr Ewan Lawson, Royal United Services Institute (RUSI), United Kingdom
- Dr Herb Lin, Center for International Security and Cooperation at Stanford University, United States
- Mr Xu Longdi, China Institute of International Studies, China
- Dr Angelos Marnerides, University of Glasgow, United Kingdom
- Prof Ciaran Martin, University of Oxford, United Kingdom
- Ms Mihoko Matsubara, NTT Comrporation, Japan
- Dr Marie Moe, SINTEF and Norwegian University of Science and Technology (NTNU), Norway
- Ms Folake Olagunju Oyelola, ECOWAS
- Mr Lukasz Olejnik, Independent security and privacy researcher and advisor, Belgium and United Kingdom
- Ms Arina Pazushko, BI.ZONE, Russia
- Prof. Adrian Perrig, ETH Zurich, Switzerland
- Mr Giacomo Persi Paoli, UNIDIR
- Ms Coralie Romet, Cyber Peace Institute, Switzerlandc
- Mr Tomslin Samme-Nlar, ICANN, Cameroon
- Mr Matthias Schulze, SWP Berlin, Germany
- Dr Haya Shulman, Fraunhofer SIT, Germany
- Ms Eva Telecka, Director, IT Security & Risk Management, Merck, Czech Republic
- Ms Noëlle van der Waag, Cowling, Security Institute for Governance and Leadership in Africa, Stellenbosch University, South Africa
- Mr Ben Wagner, TPM, TU Delft, Faculty of Technology, Policy and Management, Austria

GENEVA ACADEMY

- Prof. Robin Geiß, Director, UNIDIR
- Dr Henning Lahmann, Post-Doctoral Global Fellow, New York University

- Dr Chiara Redaelli, Research Fellow, Geneva Academy of International Humanitarian Law and Human Rights

INTERNATIONAL COMMITTEE OF THE RED CROSS

- Mr Benjamin Charlier, Legal Adviser, Arms and Conduct of Hostilities Unit
- Dr Neil Davison, Scientific and Policy Adviser, Arms and Conduct of Hostilities Unit
- Mr Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit
- Dr Kubo Mačák, Legal Adviser, Arms and Conduct of Hostilities Unit
- Dr Tilman Rodenhäuser, Legal Adviser, Arms and Conduct of Hostilities Unit
- Ms Delphine van Solinge, Digital Threats Adviser, Protection Division
- Mr Ruben Stewart, Military and Armed Groups Adviser, Unit for Relations with Arms Carriers

ANNEX 2: GUIDING QUESTIONS

I. POTENTIAL HUMAN COST OF CYBER OPERATIONS: RECENT TRENDS

The aim of these questions is to analyse the recent evolution of cyber operations and update the in-depth analysis of the potential human cost of cyber operations previously done by the ICRC.

1. What are the trends in the recent evolution of exploits and malware? What is the evolution over the last few years in terms of the type of operations and tools used (e.g. tailored for specific operations or generic in nature), the actors involved, the circumstances, the defense-offense balance? Are risks of high-impact cyber operations increasing (more, new or emerging actors, more capabilities) or decreasing (more resources for cyber security, better security posture, more resilient systems) and how does this recent evolution affect the prospective assessment of future threats?

2. Looking at specific sectors in particular: a. What are the trends in the recent evolution of the risks that cyber attacks pose to the **healthcare sector**? In particular, how has the ongoing COVID-19 pandemic affected the vulnerability and/or the resilience of the healthcare sector to cyber harm?

b. What are the trends in the recent evolution of the risks that cyber attacks pose to **critical civilian infrastructure** other than the healthcare sector, in particular cyber attacks against, or affecting energy, water, transportation, logistics, dams, nuclear plants, or chemical and biological industries?

c. What are the trends in the recent evolution of the risks that cyber attacks pose to **core internet services**, such as Internet Exchange Points (IXPs), the Domain Name System (DNS), or Certificate Authorities (CAs)? In particular, how resilient are the various components of the internet core and what is the risk that cyber attacks against such components would cause significant negative impact?

II. SOCIETAL RISKS OF CYBER OPERATIONS

The aim of these questions is to broaden the analysis to other risks that cyber operations pose to societies, such as the risk posed by cyber operations to the functioning of government services, financial services, the economy, communications, education, and to other essential civilian data, as well as the risks posed by information operations.

3. What is **of most concern** in terms of the risk of harm to people and societies posed by cyber operations (worst-case scenario, type of risk, circumstances and aim of use, likelihood, seriousness of the impact)?

4. Are **some societies more vulnerable to certain types of cyber operations**? What factors play a role (technological, cultural, political)?

5. What **sectors of society are particularly vulnerable** to hostile cyber operations? Would interference with certain (critical) infrastructures / sectors of society potentially cause systemic risks at the societal level? Which cyber components are so important from a systemic/societal perspective that they should never be interfered with and how do you distinguish them from others?

6. How do digital technologies influence or change the use of **information operations** by States and other actors (such as propaganda, mis- and disinformation, hate speech)? What risk do such operations pose to people and to societies?

7. How do we establish a reliable way to **measure the impact** of cyber operations on society? What are the criteria?

III. MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

The aim of these questions is to refine the analysis by focusing on situations of armed conflicts, including to what extent cyber operations, their use and their consequences for civilians or society might differ during peacetime and during armed conflicts.

8. How do you expect the **development and use of cyber military capabilities** to evolve in the medium- to long-term period?

9. How might the conduct of hostile cyber operations **differ during peacetime and during armed conflicts**? In particular, what are the differences in terms of the purpose of such operations (e.g. gaining access, generating effects, etc.), of their use (e.g. number, likelihood, etc.), and of their consequences for civilians or society (e.g. type, seriousness, and likelihood of causing harmful consequences) in situations of peace and during armed conflicts?

10. Strategically and operationally, **what will States/armed actors want to achieve in and via cyberspace in times of armed conflict**? What does it mean to seek supremacy in cyberspace (from a technical perspective, risks involved, etc.)? What does it mean to achieve cyber supremacy or to dominate this domain?

11. What might **cyberwarfare** (understood for the purpose of the discussion as sustained military engagement in cyberspace by sophisticated actors) look like **in the near future**? How would such engagement differ between symmetrical situations (including in so-called near-peer conflicts) and asymmetrical situations (such as in conflicts between a cyber power and a less developed State or a non-State armed group)?

IV. OTHER ISSUES OF CONCERN

12. Is there anything of significance to the theme of the workshop missing from the questions above or the contemporary debates in general? Are there possible effects that should be discussed more prominently? Do the uses of cyberspace and cyber operations create specific risks and protection needs that are omitted from contemporary discussions and need to be addressed?

ANNEX 3: BACKGROUND DOCUMENT

The project "Digitalization of Conflict: Humanitarian Impact and Legal Protection", a joint endeavour between the International Committee of the Red Cross and the Swiss IHL Chair at the Geneva Academy of International Humanitarian Law and Human Rights, aims to explore humanitarian consequences and protection needs caused by the digitalization of armed conflicts and the extent to which these needs are addressed by international law, especially international humanitarian law (IHL).

The digitalization of armed conflict is a dynamic process that encompasses the increasing use of digital means and methods of warfare based on a range of rapidly evolving technological developments, most notably in the area of cyber and other digital technologies, artificial intelligence, machine learning, sensor systems, and robotics. The project considers the effects of these developments individually and in combination with a view to assessing the risks that they entail for conflict-affected populations and ensuring that the legal and policy framework provides adequate humanitarian protection in contemporary and future warfare. The first phase of the project tackles questions in relations to cyber technologies in a military context.

New technologies have a profound impact on how wars are fought. IHL is applicable to all technological developments in warfare. The speed, scale, and transformative impact of today's extraordinary technological advances and the continuous merger of the physical and digital domains, however, require a constant (re-)assessment whether new means and methods of warfare are compatible with existing IHL rules and whether IHL continues to provide the level of humanitarian protection it is meant to ensure in times of armed conflict.

This joint initiative adopts a multi-disciplinary perspective that takes into consideration the interrelated technical, military, ethical, policy, legal and humanitarian aspects to address three overarching questions:

1. What risks, potential humanitarian consequences, and protection needs for conflict-affected populations arise on the digital battlefield?

2. Does international law, in particular IHL, adequately address these risks and protection needs?

3. If not, what recommendations could be developed in terms of law and policy beyond the existing IHL framework to mitigate these risks and address these protection needs?

With a focus on military uses of cyber technologies, the workshop will address these issues in consultation with a range of eminent experts from different relevant academic and practical backgrounds.

The overarching objective for the workshop, which is the first step in a series of events, is to provide an updated risk and protection needs assessment in view of contemporary military cyber capabilities. To this end, the workshop is divided into three sections:

(I) Potential Human Cost of Cyber Operations: Recent Trends;

(II) Societal Risks of Cyber Operations;

(III) Military Cyber Operations during Armed Conflicts.

To facilitate the discussions, this background document briefly provides essential information on these three subject areas.[*]

I. POTENTIAL HUMAN COST OF CYBER OPERATIONS: RECENT TRENDS

In recent years, the ICRC has deepened its assessment of the risks posed by cyber operations and how to avoid incidental harm in military cyber operations. In particular, the ICRC carried out an in-depth analysis of the potential human cost of cyber operations, focusing on the risk that cyber operations may result in death, injury or physical damage, affect the delivery of essential services to the population, or affect core internet services. The first section of the workshop aims to update and refine the analysis and understanding of the potential humanitarian impact of cyber operations especially in light of technological developments since the ICRC's initial study was first undertaken.

Societies have become largely dependent on digital information and communication technologies, a process only accelerated by the ongoing COVID-19 pandemic. While the benefits and opportunities are countless, increased dependency also implies increased vulnerability. Whereas the emergent proliferation of cyber tools and their use as a means or method of warfare offers militaries the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the potential human cost of cyber operations must not be neglected. By means of cyber operations, processes controlled by computer systems can be triggered, altered, or otherwise manipulated. The interconnectivity that characterizes cyberspace means that whatever has an interface with the Internet can be affected by cyber operations conducted from anywhere in the world. A cyber operation against a specific system may have repercussions on various other systems, regardless of where those systems are located.

There is a real risk that cyber tools – either deliberately or by mistake – may cause large-scale and diverse effects on critical civilian infrastructures, such as essential industries, telecommunications, transport, governmental, and financial systems. Cyber operations conducted over recent years – primarily outside armed conflicts – have shown that malware can spread instantly around the globe and affect civilian infrastructure and the provision of essential services.[26] As one cybersecurity expert put it recently, such military operations constitute a "humanitarian crisis in the making".[27]

Cyber operations can harm infrastructure in at least two ways. First, they can affect the delivery of essential services to civilians, as has been shown with cyber operations against electrical grids and the health-care sector. Second, they can cause physical damage, as was the case with the Stuxnet attack against a nuclear enrichment facility in Iran in 2010, and an attack on a German steel mill in 2014.

The health-care sector has become particularly vulnerable, moving towards increased digitization and interconnectivity without improving cybersecurity accordingly. As a result, hospitals and other health-care facilities have become frequent targets of malicious operations, in

[*] This background document aims to provide relevant material and food for thought to support the discussions during the Experts' meeting. It does not necessarily reflect the views or positions of the International Committee of the Red Cross.

[26] Examples include the malware CrashOverride, the ransomware WannaCry, the wiper program NotPetya, and the malware Triton. CrashOverride affected the provision of electricity in Ukraine; WannaCry affected hospitals in several countries; NotPetya affected a very large number of businesses; Triton was aimed at disrupting industrial control systems, and was reportedly used in attacks against Saudi Arabian petrochemical plants. For some discussion, see Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation", *Humanitarian Law and Policy Blog*, 14 November 2018.

[27] Sergio Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", *Humanitarian Law and Policy Blog*, 3 December 2019.

particular since the beginning of the pandemic. Cyber operations against other critical civilian infrastructure, such as electricity, water and sanitation, can also cause significant harm to humans by triggering physical effects. The main reason for this is that such infrastructure is often operated by industrial control systems (ICSs), which are vulnerable to malicious operations through cyberspace. A cyber operation against an ICS requires specific expertise and sophistication, and often, custom-made malware. While ICS attacks have been less frequent than other types of cyber operations, their frequency is reportedly increasing, and the severity of the threat has evolved more rapidly than anticipated only a few years ago.[28] Experts have urged the international community of IT security specialists, governments, and humanitarian lawyers to start discussing how to regulate such cyber-physical operations due to their potential to have kinetic effects and result in casualties.[29]

Moreover, the characteristics of cyberspace raise specific concerns. For example, cyber operations entail a risk for escalation and related human harm for the simple reason that it may be difficult for the targeted party to know whether the attacker's aim is intelligence collection (computer network exploitation, CNE) or more harmful effects (computer network attack, CNA). The target may thereby react with greater force than necessary out of anticipation of a worst-case scenario. Cyber tools also proliferate in a unique manner. Once used, they can be repurposed or reengineered and thus widely used by actors other than the one that had developed or used them initially. A further concern is the difficulty to reliably attribute cyber operations, which hampers the possibility to identify actors who violate international law in cyberspace and hold them responsible. The perception that it will be easier to deny responsibility for such operations may also weaken the taboo against their use – and may make actors less scrupulous about using them in violation of international law.[30]

While cyber operations to date have mostly caused significant economic damage instead of major harm to humans, much is unknown in terms of technological evolution, the capabilities and the tools developed by the most sophisticated actors – including military ones – and the extent to which the use of cyber operations during armed conflicts might be different from the trends observed so far. In other words, although the risk of human cost does not appear extremely high based on current observations, especially considering the destruction and suffering that conflicts always cause, the evolution of cyber operations requires close attention due to existing uncertainties and the rapid pace of change.

II. SOCIETAL RISKS OF CYBER OPERATIONS

This section is based on two forthcoming Geneva Academy working papers focusing on "Society Protection" and on "Protecting the Information Space in Times of Armed Conflict".

The risks for society posed by military cyber conduct go beyond potential physical damage or harm to life and limb of the civilian population. A growing number of States and international organizations have affirmed that military cyber operations against the enemy conducted during armed conflict are subject to IHL. The fact, however, that these rules were conceived and drafted long before the emergence of offensive cyber technologies raises the question whether the existing legal safeguards are sufficient for future cyber conflicts in regard to the protection of societies that may be adversely affected by these new capabilities in novel and hitherto inconceivable ways. The

[28] Laurent Gisel and Lukasz Olejnik (eds), *ICRC Expert Meeting: The Potential Human Cost of Cyber Operations*, ICRC, Geneva, 2019, p. 25.

[29] Marina Krotofil, "Casualties Caused through Computer Network Attacks: The Potential Human Costs of Cyber Warfare", 42nd Round Table on Current Issues of International Humanitarian Law, 2019, p. 8.

[30] ICRC, International humanitarian law and the challenges of contemporary armed conflicts, 2011, p. 37; ICRC, International humanitarian law and the challenges of contemporary armed conflicts, 2019, p. 20.

existing rules of IHL were originally conceived with an entirely different type of hostilities in mind. Their general scope and underlying assumptions were tailored towards the physical effects of the conduct of hostilities and focused on the mitigation of suffering brought about by physical violence as traditionally understood. It is thus less clear whether they can effectively regulate the full spectrum of modern conflicts involving cyber means and sufficiently constrain the belligerent parties.

In view of today's military cyber capabilities, it might thus be inquired whether a new, additional dimension of disruptive consequences and resultant legal protection needs is emerging. This dimension relates to the impacts that military cyber operations can have on the functionality of essential societal processes across economic, financial, scientific, cultural, and healthcare sectors as well as with regard to public opinion formation and other public sectors. Such operations could include the paralysation of a country's administration nation-wide, the encryption of tax records of thousands or millions of citizens, the breaking down of communal services like water, electricity, or garbage disposal, or the disruption of financial markets or supply chains on a large scale. While these impacts may be more diffuse and intangible and more difficult to measure than war casualties or physical destruction caused directly by kinetic means of war, in an increasingly interconnected world they can affect entire societies and cause systemic disruption. Traditionally, some of these impacts such as economic losses without a link to specific attacks or psychological operations not amounting to prohibited acts or threats of violence with the primary purpose of spreading terror among the civilian population nor to encouragement of IHL violations would have been considered as falling outside the regulatory ambit of IHL.

In that sense, it should be discussed whether modern cyber conflict can be considered a paradigm shift, as serious and lasting disruptions of civil society are increasingly a reality even without the infliction of any physical damage. In the long run, these developments may come to be seen as a mere starting point to a more fundamental change in warfare. With a rapid technological evolution and ever-increasing interdependencies and attack surfaces across all societal domains, in the long run there is a real risk of a gradual undermining if not a reversal of the fundamental understanding that the civilian population must not be targeted in times of armed conflict. Adopting narrow interpretations that would limit the scope of IHL rules concerning the conduct of hostilities to physical manifestations of violence and damage, would risk leaving essential aspects of civilian life and essential parts of the civilian infrastructure unprotected and vulnerable to direct attacks in the 21st century.

For this reason, it might be asked whether contemporary warfare calls for a more comprehensive understanding of what protection of the civilian population entails; an understanding that takes into account the central importance of various societal processes. Interestingly, in the realm of peacetime international law, some states appear to be more readily prepared to include new dimensions of protection that accept non-physical effects on digital and a wide range of societal processes (economic, financial, cultural) as falling within the scope of concepts such as sovereignty, non-intervention, or the use of force. Considering the rapid evolution of military cyber capabilities and resources, more discussion is needed within the context of IHL as well with regard to economic, financial, or other societal processes. What seems increasingly crucial is not only the civilian population in and of itself, i.e. the natural persons and their physical assets directly at risk from harm, but systemic societal processes writ large whose disruption will entail serious repercussions for the civilian population in its entirety. Moreover, certain states and other stakeholders have expressed views in support of interpretations that would permit far-reaching operations against societies during armed conflict.

The challenge ahead, then, is to see whether, and to what extent, the existing legal framework of IHL might need strengthening, without overstretching this legal regime's protective reach that by its very nature must take into account the military necessities and realities of war. The primary question is whether certain societal processes and functions must be considered as important and essential enough to require legal protection under IHL in times of armed conflict. Against this backdrop, the workshop aims to discuss whether IHL, as it currently stands, sufficiently protects the various societal dimensions and processes that could be affected by (sophisticated) cyber operations. We are therefore seeking input and expertise from the workshop participants, on the various ways in which cyber operations could affect essential societal processes, also and especially, beyond the more obvious effects such as the infrastructure disruptions that are commonly discussed.

III. MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

This section is based on a forthcoming ICRC report and a recent article in the International Review of the Red Cross written by three ICRC lawyers.

The use of cyber technology has become a reality in today's armed conflicts and is likely to increase in the future. Some States have acknowledged publicly that they have conducted cyber operations in ongoing armed conflicts. In particular, the United States, the United Kingdom, and Australia have disclosed that they used cyber operations in their conflict against the Islamic State group.[31] There are also public reports suggesting that Israel used cyber operations against Hamas – and allegations that Hamas used cyber operations against Israel.[32] Furthermore, cyber operations have affected other countries involved in armed conflicts, such as Georgia in 2008,[33] Ukraine in 2015–17,[34] and Saudi Arabia in 2017,[35] though the authors of these cyber operations remain unknown and attribution of responsibility is contested. It is therefore unclear whether these operations had a nexus to the respective armed conflicts and thus whether IHL applied. Moreover, there have been reports of cyber operations by States in other situations where the legal classification may not be straightforward, including in what is sometimes referred to as a "grey zone".[36] These examples show an increase in military cyber operations over the past decade – a change in warfare that might continue. Indeed, an increasing number of States are said to have or to be developing cyber military capabilities, including the five permanent member States of the UN Security Council.[37] It has been argued by some researchers that over 100 States have military

[31] See, in particular, Mike Burgess, Australian Signals Directorate, "Offensive Cyber and the People Who Do It", speech given to the Lowy Institute, 27 March 2019; Paul M. Nakasone, "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services", 14 February 2019; Jeremy Fleming, GCHQ, "Director's Speech at CyberUK18," 12 April 2018.

[32] "Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions", *BBC News*, 15 May 2019; Zak Doffman, "Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First", *Forbes*, 6 May 2019.

[33] David Hollis, "Cyberwar Case Study: Georgia 2008", *Small War Journal*, 2010, available at: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[34] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 22 August 2018.

[35] Blake Johnson et al., "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", *Fireeye Blogs*, 14 December 2017.

[36] For example, there have been various media reports – based on anonymous official sources – that the United States has carried out cyber operations against targets in Russia and Iran, and that Israel has carried out a cyber operation against a port in Iran. See Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms", *Washington Post*, 27 February 2019; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", *New York Times*, 15 June 2019; Julian E. Varnes and Thomas Gibbons-Neff, "U.S. Carried out Cyberattacks on Iran", *New York Times*, 22 June 2019; Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility", *Washington Post*, 18 May 2020.

[37] In addition to the United States and the United Kingdom, France has set out the objective of "acquir[ing] a cyber defence capability" to defend against "foreign States or terrorist groups [which] could attack the critical infrastructures". France, Agence Nationale de la Sécurité des Système d'Information, *Information System Defence and Security: France's Strategy*, 2011. The 2015 *White Paper on China's Military Strategy* states that "in response to the increasing development of cyber military capabilities from other states, China will develop a defensive cyber military capacity". See Government of China, *White Paper on China's Military Strategy*, 2015. Russia has been less explicit on the subject, but the Russian Federation's *Doctrine of Information Security* identifies "upgrading the information security system of the Armed Forces of the Russian Federation, other troops, military formations and bodies, including forces and means of information

cyber organizations, although these take a range of forms and have a range of responsibilities.[38] Against this background, from a humanitarian perspective it is imperative to inquire in what ways cyber military capabilities might be further developed and used in the medium to long term.

In this context, it should additionally be considered how the conduct of cyber operations during armed conflict is different from those carried out during peacetime. Broadly speaking, State militaries have responsibility for three main tasks in cyberspace. Firstly, they are responsible for defending military networks from intrusions from the full range of threat actors, from the inquisitive teenage hacker, through hacktivists and criminals, to other States and their militaries. As military capabilities continue to be connected and networked, the opportunity for adversaries to target vulnerabilities in those networks to disrupt or disable military capabilities becomes increasingly significant. In some States, that responsibility for defence of military networks is extended to the provision of support to the wider critical national infrastructure, particularly in a time of crisis. The second task is the traditional military function of intelligence collection and analysis focused on potential adversaries. The role of the military in national intelligence collection is varied with responsibilities sometimes being shared with civilian intelligence agencies, but armed forces have a continuing need to collect information on the battlefield at the very least. It is in this context that it is necessary to clearly distinguish between the use of military cyber capabilities during peacetime from those during situations of armed conflict in terms of, *inter alia*, their purpose and mode of conduct. Thirdly, some military cyber organizations have been tasked with the projection of national power in and through cyberspace through offensive cyber operations during armed conflict. These can be conducted against targets from the strategic to the tactical level including adversary weapons systems, command and control networks or logistics hubs. Ultimately, the purpose is to create physical and/or cognitive outcomes that contribute to achieving the objectives of the military campaign and as such are increasingly integrated into the planning and execution of military operations. Here, too, future discussions would benefit from a precise analysis of the particularities of State cyber conduct during armed conflict as opposed to operations during peacetime, not least in regard to quality and gravity of harmful consequences.

Examples of the use of offensive cyber operations during conflicts include espionage; target identification; information operations to affect the enemy's morale and will to fight; the interruption, deception or obfuscation of the enemy's communication systems aimed at hindering force coordination; and cyber operations in support of kinetic operations.[39] An example of the latter is the disabling of an enemy's military radar stations in support of air strikes.[40] This non-exhaustive list raises the question concerning possible strategic and tactical objectives that militaries might want to achieve by means of cyber conduct in armed conflict in order to gain a deeper understanding of the future of cyber conflict. In particular, it is necessary to explore in more detail what "cyber warfare" in a narrower sense could look like in the near-term future, understood as sustained military confrontation between sophisticated actors "in" cyberspace, and how such scenarios might play out differently depending on whether a military faces a symmetrical or an asymmetrical conflict situation.

confrontation" as a "key area of ensuring information security in the field of national defence". See Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, 5 December 2016.

[38] Shachtman Noah and Peter W. Singer, The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive, Brookings Institute, Washington DC, 2011.

[39] ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts, forthcoming.

[40] Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", *Wired*, 4 October 2007; Lewis Page, "Israeli Sky-Hack Switched Off Syrian Radars Countrywide", *The Register*, 22 November 2007.

The Geneva Academy of International Humanitarian Law and Human Rights

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

The Geneva Academy of International
Humanitarian Law and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch

Filename:	6643EB26.docx
Directory:	C:\Users\avanthat\AppData\Local\Microsoft\Windows\INetCache\Content.MSO
Template:	W:\Publications\Briefings - In-Briefs - Policy Briefings - Research Briefs\Working Papers\Template\Working Paper Template.dot
Title:	
Subject:	
Author:	Tatiana Avanthay
Keywords:	
Comments:	
Creation Date:	18/03/2021 15:25:00
Change Number:	91
Last Saved On:	20/06/2022 15:31:00
Last Saved By:	Avanthay Tatiana
Total Editing Time:	325 Minutes
Last Printed On:	21/06/2022 09:11:00
As of Last Complete Printing	
Number of Pages:	35
Number of Words:	19'079 (approx.)
Number of Characters:	108'755 (approx.)