ICRC EXPERT MEETING
21–22 JANUARY 2020 – GENEVA

AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

REPORT

COMITE INTERNATIONAL GENEVE

ICRC

ICRC EXPERT MEETING
21–22 JANUARY 2020 – GENEVA

AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

REPORT PREPARED BY EWAN LAWSON, MILITARY ADVISER ON CYBER,
AND KUBO MAČÁK, LEGAL ADVISER, ICRC

CONTENTS

ACKNOWLEDGEMENTS 4

FOREWORD 5

EXECUTIVE SUMMARY 6

INTRODUCTION 8

Purpose and scope of the meeting 8

Structure of the report 9

1. CYBERSPACE AS A CONTESTED ENVIRONMENT 10

A. Cyberspace as a domain 10

B. Competition in cyberspace and its limits 11

Key takeaways 12

2. THE ROLE OF THE ARMED FORCES IN CYBERSPACE 13

A. Actors 13

B. Roles and responsibilities 14

C. Grey zones 15

Key takeaways 15

3. MILITARY CYBER OPERATIONS 16

A. Typology of military cyber operations 16

B. Conduct of military cyber operations 17

C. Development of military cyber capabilities 18

Key takeaways 18

4. ASSESSING THE RISK OF CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS 19

A. Understanding the risk of civilian harm 19

B. Assessing the risk of civilian harm 20

Practical application 22

Key takeaways 24

5. MEASURES TO AVOID OR REDUCE CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS 25

A. Ownership of risk – attackers and defenders 25

B. Precautions in attack 26

C. Precautions against the effects of attacks 27

D. Legal and policy preventive measures 28

Practical application 30

Key takeaways 31

6. FUTURE DEVELOPMENTS IN MILITARY CYBER OPERATIONS AND THEIR IMPACT ON THE RISK OF CIVILIAN HARM 32

A. Artificial intelligence and autonomy 32

B. Internet of Things and quantum computing 33

C. The developing nature of military cyber operations 34

Key takeaways 35

ANNEX 1: BACKGROUND DOCUMENT 36

ANNEX 2: SCENARIOS 55

ANNEX 3: LIST OF EXPERTS 58

ACKNOWLEDGEMENTS

The present report is the outcome of an expert meeting held in January 2020 on avoiding civilian harm from military cyber operations.

The conceptualization, drafting and publication of the report would not have been possible without the commitment and contributions of many individuals.

Our gratitude goes, first of all, to the experts who participated in a personal capacity and whose expertise, knowledge and contributions were essential for the success of this meeting. They shed light on the various aspects of the conduct of military cyber operations, including the assessment of the risk of civilian harm and the procedures and practices that might be employed to mitigate that risk.

We would also like to express our gratitude to Ewan Lawson, Military Cyber Adviser, who was in charge of organizing the meeting and drafting the background document; Kubo Mačák, Legal Adviser, who co-authored this report with Ewan Lawson; and Laurent Gisel, then Senior Legal Adviser and Cyber team leader, who supported the organization of the meeting and the drafting of the background document.

We would further like to extend our thanks to: Lindsey Cameron, Head of the Thematic Legal Advice Unit, Neil Davison, Scientific and Policy Adviser, Jonathan Horowitz, Legal Adviser, and Tilman Rodenhäuser, Legal Adviser, who contributed to the drafting of the report through their comments, provided valuable support in the organization and follow-up of the expert meeting or helped with the publication of the report; Giulia Carlini, Zoi Lafazani and Giorgio Macor, Associates, who assisted in the preparation of this report.

Cordula Droege
Chief Legal Officer and Head of the Legal Division, ICRC

FOREWORD

In recent years, cyber operations have shown that the functioning of critical civilian infrastructure – hospitals, power grids and even nuclear plants – is at risk of disruption through cyber means. A few States have publicly acknowledged using cyber operations during armed conflicts, and a growing number of States are developing military cyber capabilities.

Under international humanitarian law (IHL), the civilian population must be protected against the dangers arising from military operations. However, there is little consensus around the question of how IHL protects civilians against the effects of military cyber operations during armed conflicts.

Most known cyber operations thus far have been conducted outside armed conflict and there is very little transparency about the use of cyber capabilities by armed forces. Developing an understanding of the practical issues for the implementation of IHL in military cyber operations therefore remains a significant challenge.

To move towards a realistic appreciation of the practical issues for the implementation of IHL in military cyber operations, the International Committee of the Red Cross (ICRC) invited experts from various parts of the world to share their knowledge. Participants included experts with experience in the development and use of military cyber operations, experience working for global IT companies and cyber threat intelligence firms, as well as lawyers and academics. Experts analysed the conduct of military cyber operations, focusing on how armed forces can understand and assess the risk of civilian harm and what measures might be effective and appropriate to avoid or mitigate such risks.

The rich discussions provided an insightful picture of the ways in which armed forces consider the application of IHL when conducting cyber operations and the risks that such operations can entail for the civilian population. What emerges from the discussions is that States need to invest time and resources to develop tools, processes to assess the risks of incidental civilian harm and measures to limit these risks.

We are grateful to the experts for having shared their deep knowledge and expertise. With this report, we hope to contribute to a better understanding of the conduct of military cyber operations and, in particular, how armed forces can, and should, consider risks to civilians and the measures to be taken to avoid and mitigate such risks.

Cordula Droege
Chief Legal Officer and Head of the Legal Division, ICRC

EXECUTIVE SUMMARY

In today's armed conflicts, cyber operations are increasingly used in support of and alongside kinetic operations. Several States have publicly acknowledged such use, and many more are developing military cyber capabilities as well as doctrines and policies that aim to establish national approaches and principles for the military uses of cyberspace.

In parallel, cyber incidents without, or with unclear, links to armed conflicts have resulted in damage and disruption to civilian services. These incidents have included cyber operations against hospitals, water and electrical infrastructure, and nuclear and petrochemical facilities. They offer a chilling warning about the potential humanitarian impact of military cyber operations in contemporary and future armed conflicts.

If the risk of civilian harm from military cyber operations is to be reduced, it is necessary to consider how it can be assessed and measured. This report presents the findings from an expert meeting convened by the ICRC in January 2020 to discuss these issues.

1. States should address the concerns posed by the increasing integration of cyber operations with other military capabilities during armed conflicts.
Modern armed forces perceive cyber operations as part and parcel of a wide range of military capabilities. These operations fulfil various purposes that can be roughly divided into exploitation, defence and offence. Such purposes are often interlinked: for example, exploitation often needs to be carried out before an offensive operation can be launched.

However, State-run cyber operations are not only conducted by the armed forces; intelligence agencies, the private sector and other actors have also been involved. To protect the civilian population and to ensure appropriate oversight, States should avoid the blurring of the functions of the organizations involved in the conduct of such operations and keep such operations under the supervision and control of the relevant authorities.

Moreover, discussions concerning the risk of civilian harm posed by such operations are made difficult by the persisting lack of clarity on terminology regarding interaction in cyberspace. Accordingly, States should work towards a shared lexicon pertaining to military cyber operations.

2. Existing processes must be adapted to the cyber context to ensure compliance with international humanitarian law (IHL).
Compared to kinetic operations, understanding the possible collateral effects of military cyber operations and the risk to civilians can be challenging because of the interconnected and dynamic nature of target systems and networks, as well as the armed forces' relative inexperience in conducting such operations.

Some States have made the basic procedures for targeting publicly available. However, the details on how these are conducted in practice tend not to be released, which is particularly the case with military cyber capabilities.

Accordingly, States should use the existing processes developed for the purposes of kinetic operations as a general frame of reference and adapt them to account for the challenges posed by cyber operations. It is essential that procedures governing such operations be IHL-compliant and, to the extent possible, transparently so.

3. States must put in place measures to mitigate the risk of civilian harm posed by the use of military cyber capabilities (also referred to as 'active precautions').
IHL mandates that in the conduct of military operations, constant care must be taken to spare the civilian population and civilian objects. In particular, cyber operators need to understand the extent to which target networks and systems are interconnected, the risk of malware spreading in unintended ways, and the risk of indirect effects.

States should have mitigation strategies in place for all military cyber capabilities they consider developing. Specifically, a variety of technical measures can be considered, such as 'system-fencing' (preventing malware from executing itself unless there is a precise match with the target system), 'geo-fencing' (limiting malware to only operate in a specific IP range), or 'kill switches' (disabling malware after a given time or when remotely activated).

However, not all military cyber operations involve the deployment of malware. In operations that consist of taking direct control of the target system, mitigation is rather a matter of establishing appropriate decision-making processes. At every stage, States should involve expertise from a wide range of sources and ensure that this is put into straightforward language for the relevant decision makers.

4. States must put in place measures to protect the civilian population against the dangers resulting from military cyber operations (also referred to as 'passive precautions').

Parties to conflicts that may be the object of cyber operations have a responsibility to minimize the risk of civilian harm posed by such operations. Some of these measures may have to be implemented already in peacetime.

In particular, States should build strong cyber resilience cultures across their societies and ensure that their critical infrastructure is protected to the best possible standard. States should also have a sufficient understanding of the critical dependencies in their networks in order to be able to restore their functionality in the event of a destructive or disruptive attack.

Moreover, armed forces tend to create distinct, dedicated military networks, to facilitate their defence. This may also limit the spread of harmful effects onto civilian networks when such a military network is attacked. Designing civilian systems such that they are not reliant on systems that may qualify as military objectives likewise reduces the risk of civilian harm.

5. States should address the risk of civilian harm posed by so-called information operations and grey-zone operations.

There is a growing trend of using digital technologies to engage in operations that spread disinformation, undermine social cohesion, or even incite violence (sometimes referred to as 'information operations').

The related notion of 'grey-zone operations' describes competition between States that appears to fall between the standard categories of peace and war. States sometimes argue that such operations offer means that are less lethal and less escalatory than traditional military operations. However, these operations may also lead to unexpected escalation and thus considerable civilian harm, depending on how they are perceived by the adversary.

Accordingly, States and other stakeholders should work towards a better understanding of the risks posed by information and grey-zone operations. In addition, States should ensure that all organizations involved in the conduct of military cyber operations (including, but not limited to the armed forces and intelligence agencies) are acquainted with the scope of application and requirements of IHL.

6. States and other stakeholders should continue to develop their understanding of the risk of civilian harm posed by new technologies and work towards mitigating those risks.

In the future, advances in artificial intelligence (AI) will likely be integrated into military cyber capabilities, leading to a degree of operational autonomy and thus to new risks of civilian harm. In addition, the growth of the Internet of Things (IoT) will expand the attack surface and the range of vulnerabilities available to be exploited by malicious actors. Finally, quantum computing will boost available computational power by orders of magnitude, resulting in unprecedented growth in the volume and speed of data processed by computers.

Accordingly, States should ensure that in the deployment of autonomous cyber systems, commanders or operators always retain a level of human control sufficient to allow them to make context-specific judgements to apply IHL. States and other stakeholders should also continue to study the risks associated with the expansion of the IoT and with the quantum-enabled increase in the speed and scale of cyber and other operations.

INTRODUCTION

While most reported cyber operations[1] do not have an apparent connection to an armed conflict, a few States have acknowledged their use in that context. Those States and others have publicly declared that their armed forces are developing capabilities, doctrine and operating procedures for conducting military operations in and through cyberspace.

Precise definitions of the term 'cyberspace' remain contested; however, for the purposes of this expert meeting, it was taken to refer to the physical, virtual and cognitive spaces created by the global interconnectedness of information and communications technologies. The creation of cyberspace is directly linked to the digital 'revolution' or 'transformation', which has altered many aspects of the ways in which societies interact.

These changes have enabled the transmission of information in near real time and in quantities that had not been previously possible. The new technologies provide immense opportunities for social and economic development at local, regional and global levels. However, at the same time, cyberspace has also become a venue for competition and conflict as States and other actors seek to maximize the potential benefits to themselves and limit them to others.

PURPOSE AND SCOPE OF THE MEETING

As part of its mandate to work for the understanding and dissemination of knowledge of IHL and, if necessary, prepare any development thereof,[2] the ICRC monitors the development of new technologies that are, or could be, used as means and methods of warfare during armed conflicts. This approach is based on legal, military, technical, ethical and humanitarian considerations, which are closely related.

Under IHL, States have an obligation to take constant care to spare the civilian population, civilians and civilian objects from the dangers resulting from military operations.[3] All feasible precautions must be taken to avoid or at least minimize incidental civilian harm when carrying out attacks, including, in the ICRC's view, through cyber means and methods of warfare.[4] The question is how this is or should be done in the conduct of military cyber operations, what can be learnt and transposed from kinetic operations, and what are the particular characteristics of cyberspace that require adapted measures to comply with IHL.

At the same time, States remain reluctant to disclose or even discuss their military cyber capabilities, including the ways in which those capabilities are employed during armed conflicts. This makes developing an understanding of the assessment and mitigation by the armed forces of the risk to civilians particularly challenging.

[1] The term 'cyber operations during armed conflicts' is used throughout the report to describe operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means and methods of warfare in the context of an armed conflict. Cyber operations rely on information and communication technologies. For a specific discussion of the challenge of defining military cyber operations, see Chapter 3 below.

[2] *Statutes of the International Red Cross and Red Crescent Movement*, Art. 5, available at: https://www.icrc.org/en/doc/assets/files/other/statutes-en-a5.pdf.

[3] See Article 57 of the 1977 First Additional Protocol; J-M. Henckaerts and L. Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. I: Rules*, ICRC, Cambridge University Press, Cambridge, 2005 (hereinafter ICRC Customary IHL Study), Rule 15.

[4] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts – ICRC position paper', November 2019, p. 6.

With this expert meeting, the ICRC sought to better understand how armed forces assess the risk of civilian harm, and which procedures and practices they employ or should employ to mitigate that risk. The meeting included participants with practical experience in carrying out military cyber operations, cyber security strategists and analysts, and academics with relevant expertise.

The meeting focused on military cyber operations during armed conflicts, in particular those that are carried out by States' armed forces, but it was emphasized that other State organs – such as intelligence agencies – are also often involved. While some of the discussions, analysis and findings may be equally relevant for the use of cyber operations by non-State parties to armed conflicts, the specific issues that the latter might raise were outside the scope of the meeting.

STRUCTURE OF THE REPORT

The report begins by exploring the nature of cyberspace as a contested environment in which military cyber operations are conducted (Chapter 1). It then focuses on the role of the armed forces in cyberspace and examines the range of potential military cyber operations (Chapters 2 and 3). This is followed by an analysis of the ways in which armed forces assess and mitigate the risk of civilian harm from such operations (Chapters 4 and 5). Finally, the report considers how military cyber operations might develop in future and what impact these developments may have on the attendant risk of civilian harm (Chapter 6). Each chapter concludes with the ICRC's key takeaways from the discussions.

The expert meeting was organized around specific topics, using a detailed background paper (Annex 1) and a set of hypothetical scenarios (Annex 2), both prepared by the ICRC in advance of the meeting. While the various points made in the discussion summarized here are not attributed to the experts who made them, a list of participants is provided (Annex 3). An earlier draft of the present report was submitted to experts for comments prior to its publication.

Neither this report nor any of the annexes necessarily represent the views of the ICRC.

1. CYBERSPACE AS A CONTESTED ENVIRONMENT

This chapter sets the scene for the rest of the report by examining the nature of the space in which military cyber operations are conducted. It details how cyberspace today is understood as a contested environment and explores how competition in that domain, particularly between States, manifests itself. The chapter highlights different understandings of cyberspace and its relationship with the so-called 'information space'. Finally, it discusses the ways in which interstate competition in cyberspace occurs and the law and policy-related limits on these forms of competition.

A. CYBERSPACE AS A DOMAIN

The expert meeting underscored the ubiquity and essential nature of cyberspace to contemporary States and societies across the globe. One expert described cyberspace as 'a new kind of oxygen' to emphasize its importance at all times, as a venue used both for cooperation and for conflict. It was noted that some States had specifically identified cyberspace as a new domain of warfare, but also that this designation was not universally accepted. Overall, the discussions confirmed the persisting lack of clarity on terminology regarding State interaction in cyberspace.[5]

When considering power relationships in the international system, States now consider their 'cyber power' as much as more traditional measures of State power and influence. As noted by one of the experts, "to be a global power, one must be a global cyber power". Still, the extent to which States are able to benefit from, and control, cyberspace reflects the resources at their disposal. Several experts argued that some of the more advanced States were seeking to control cyberspace, particularly through the provision of critical digital infrastructure, and that this is reflected in debates about how cyberspace should be regulated and governed.

Experts also noted that the competition in cyberspace impacted directly on small and medium-sized States. These States needed to be conscious of their dependency on others to be able to utilize cyberspace for the benefit of their societies. In this connection, one of the experts warned of the creeping trend of 'digital colonization': the growing risk that dependency on the provision of digital services by outside States reduces the control that technologically less-developed States may have within their own territories.

Another key concept that is gaining increasing traction is the notion of 'digital sovereignty', which reflects the idea that States should assert their authority over the internet and protect their citizens and businesses from cyber harm.[6] Experts noted that States, societies and individuals are dependent on others not just for their digital infrastructure but also for the storage of their data. This has led some States to consider ways to ensure they are able to maintain their digital sovereignty, as highlighted, for example, by Estonia's establishment of digital embassies[7] and Russia demonstrating an ability to disconnect from the global internet.[8] Some experts expressed concern that this could lead to a fragmentation of cyberspace by governments into national and regional networks, also referred to as the 'splinternet' phenomenon.

[5] For further discussion of this topic, including existing definitions, see Section I of the background document contained in Annex 1.

[6] Julia Pohle and Thorsten Thiel, 'Digital sovereignty', *Internet Policy Review*, Vol. 9, No. 4, December 2020, pp. 1–19, at 2.

[7] See e-Estonia, "Data Embassy".

[8] See C. Cimpanu, "Russia successfully disconnected from the internet", ZDNet, 23 December 2019.

There is an overlap between cyberspace and what might be labelled the 'information space', although there is no agreement on the exact contours of that conceptual overlap, which in turn impedes the discussion between States about the relevant threats and challenges. In this regard, experts underscored the growing concern about the impact of disinformation and propaganda and how this might cause harm to civilians. For example, politically motivated actors and extremist groups have exploited social media to spread incendiary rhetoric and thus undermine social cohesion or even incite intercommunal violence. Misinformation and disinformation have also been used as recruitment tools by violent extremist groups such as the Islamic State group. Further, one expert mentioned the example of the Russian Federation's Doctrine of Information Security (2016) to highlight that States are concerned that new information threats enabled by cyberspace may challenge the security and stability of society and the State.[9] Thus, while recognizing that the focus of the meeting was on military cyber operations that might cause civilian harm that are broadly analogous to conventional kinetic operations,[10] experts agreed that cyberspace can also be instrumentalized by a variety of actors to cause other forms of harm to civilians. Similarly, while efforts are made by States to ensure resilience in the access to cyberspace for their societies, it also carries the risk of deepening the surveillance of populations.

B. COMPETITION IN CYBERSPACE AND ITS LIMITS

Cyberspace has been a venue for interstate competition and conflict for at least the past two decades. Some experts expressed concern that the identification of cyberspace as a new domain of warfare and the adoption of related definitions and concepts fed into State practice and the legitimization of warfare in cyberspace, while others considered it inevitable that States would use all available domains of activity to exert their power and influence.

Initial State activity in cyberspace was focused on espionage. This built upon traditional forms of intelligence gathering, but global interconnectedness enabled the collection of larger quantities of information, at a greater speed and distance than had been the case in the past. States then discovered the potential for the disruption of systems through cyberspace. One expert considered that cyber attacks on national critical infrastructure had become "a staple of statecraft". However, other experts noted that many States, particularly in the global South, are only just starting to develop military offensive cyber capabilities. While that may allow them to learn the technical lessons of those who have done so before, there is a risk that the absence of tried and tested doctrines and experience could cause problems in future conflicts.

All of the experts agreed that the ongoing competition in cyberspace is subject to limits found in the existing rules of international law. It was also suggested that States should manifest already in peacetime their commitment towards IHL and reaffirm its applicability to cyber operations. One expert emphasized that these rules represent "well-constructed mechanisms" and that it would be dangerous to try to reinvent a wholly new regulatory framework. However, differing views were expressed among the experts as to the need for further development of the law. One expert considered that the Tallinn Manual project and other international norm-making initiatives were a good basis for identifying the current legal framework and if, and in which direction, the law should evolve. Others noted that the Tallinn Manual did not enjoy universal support and suggested that new cyber-specific international treaties and arrangements would constitute a useful additional layer to the existing body of rules, for instance, by clarifying the applicable conceptual framework or by applying the general rules to the practicalities of the cyber domain.

With respect to hostile cyber operations, several experts suggested that military cyber operations conducted during armed conflict by responsible actors would be under the equivalent internal scrutiny for compliance with IHL as conventional kinetic operations. However, it was noted that much malicious activity by States and

[9] The Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, 5 December 2016.

[10] See note 1 above for the notion of 'cyber operations during armed conflict'.

others takes place below the threshold of armed conflict as defined by IHL.[11] Accordingly, IHL would not govern such activities, which may also render inapplicable the IHL-specific internal scrutiny processes. Overall, it was underscored that States should develop their concepts and doctrines in innovative but responsible ways in order to address the new reality of the development of military cyber capabilities. In doing so, they should be transparent and open to informed public discussion.

While not all military cyber activities necessarily risk causing civilian harm, a risk of misperception remained as to what was intended by the actor, and hence of unexpected escalation of competition and conflict. Furthermore, a cyber operation could have consequences that are unintended by the initiator, either because the initiator is reckless as to such a risk or because there has been a failure of mission and risk analysis. For instance, experts noted that some forms of malware appeared to have caused considerable damage outside their intended targets. Conversely, one expert mentioned the example of Stuxnet as a cyber capability designed in a way that minimized the risk to other systems in case it would spread outside the 'air-gapped'[12] systems of the target facility in Iran, as it did.[13]

Finally, it was noted that interstate cyber competition could be contributing to a militarization of cyberspace. Experts flagged examples of leaders describing their countries as being in a state of 'war' because they were facing frequent cyber operations against their critical national infrastructure. It was noted that this use of the language of war might wrongly suggest that the only appropriate response was a military one whereas experts agreed that there were other tools for States to use to counter this challenge, including diplomacy.

KEY TAKEAWAYS

- States should address the persisting lack of clarity on terminology regarding interaction in cyberspace, including in relation to the absence of a shared definition of the term 'cyberspace' or its overlap with 'information space'.
- States should develop their concepts and doctrines in innovative but responsible ways in order to address the new reality of the development of military cyber capabilities. In doing so, they should be transparent and open to informed public discussion.
- Without prejudice to the question of militarization of cyberspace, States should maintain the global consensus that the ongoing competition in cyberspace is subject to limits found in the existing rules of international law and work towards an affirmation by the entire international community that IHL applies to the use of cyber operations during armed conflicts.
- States should avoid using the language of war when referring to the interstate cyber competition below the threshold of armed conflict, so as not to contribute to the militarization of cyberspace.

[11] See Articles 2 and 3 common to the Geneva Conventions, and the ICRC's 2016 commentary on these articles, in particular paras 253-256 and 436-437. See also M.N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017, Rules 80, 82 and 83.

[12] The term 'air-gapping' refers to a security measure consisting of the physical isolation of a computer or a computer network in order to prevent it from connecting to unsecured networks, such as the internet or an unsecured local area network.

[13] See Section IV of the background document in Annex 1.

2. THE ROLE OF THE ARMED FORCES IN CYBERSPACE

This chapter focuses on the role of the armed forces in cyberspace. It discusses how armed forces organize for operations in cyberspace and integrate them with their other military activities. It covers the relationship between armed forces and other actors engaged in State-run cyber operations, the roles of ostensibly civilian actors in military cyber operations and the nature of the civilian oversight of military operations. Finally, it highlights the challenges raised by so-called 'grey-zone operations', referring to cyber activities by the armed forces in situations that are difficult to classify as either peace or armed conflict.

A. ACTORS

The discussions at the meeting confirmed that many States have established cyber units within their armed forces and increasingly engage in both defensive and offensive cyber operations. However, State-run cyber operations are not only conducted by the armed forces. Intelligence agencies often have a central role while the private sector and sometimes non-State actors such as 'patriotic hackers' may also be involved.

Against this backdrop, experts discussed the nature of the challenges faced by States in cyberspace and in particular the difficulty for a State targeted by a hostile cyber operation to identify whether a malicious actor is part of a foreign State's armed forces, another type of governmental agency, or a non-State actor. While the term 'advanced persistent threat' (APT) is used routinely in the cyber security industry to describe the sort of threat actor that represents a significant challenge to a State, it is not always clear whether these are military or State-sponsored entities, or non-State actors.

Many State cyber organizations are built on a mix of military and civilian personnel and capabilities. This is the case, for instance, of the Australian Signals Directorate (ASD) and the UK's Government Communications Headquarters (GCHQ).[14] In particular, ASD highlighted the role of civilian cyber operators in its operations against the Islamic State group.[15] In some States, personnel from private industry are often employed as contractors in addition to military and civilian government personnel. One expert also noted that there was evidence that some States were seeking to expedite the development of their own cyber capabilities through the employment of 'cyber mercenaries', although this had apparently so far been limited to espionage rather than effects operations.[16]

The meeting also considered the position of computer emergency response teams (CERTs). It was noted that the norms of responsible State behaviour in cyberspace adopted by the UN provide that CERTs should not be deliberately harmed by other States.[17] However, it was suggested that this protection might be affected if during an armed conflict a given CERT was protecting critical infrastructure that had become a military

[14] In November 2020, the UK announced the creation of the National Cyber Force, formed as a partnership between the Ministry of Defence and the GCHQ, and tasked with "conducting cyber operations to disrupt hostile State activities, terrorists and criminals threatening the UK's national security". See GCHQ, "National Cyber Force transforms country's cyber capabilities to protect the UK", 19 November 2020.

[15] This operation, known in the US military as GLOWING SYMPHONY, is discussed in the background document in Annex 1.

[16] The example cited was a team in the UAE which the government has stated was employed to counter violent extremism. See C. Bing and J. Schectman, "Special Report: Inside the UAE's secret hacking team of US mercenaries", *Reuters*, 30 January 2019.

[17] See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, pp. 7–8 para. 13(k). The report was later endorsed by a unanimously adopted resolution of the UN General Assembly. See UN General Assembly, Resolution 70/237, *Developments in the field of information and telecommunications in the context of international security*, adopted on 23 December 2015.

objective. It was also noted that the blurring of the functions of the organizations involved in cyber operations potentially impacted on the protection afforded to CERTs as civilian entities during armed conflicts. This is the case particularly if, as in Australia and the UK, the national CERT is part of the national cyber security centre which is, in turn, a part of the national signals intelligence agency (ASD and GCHQ, respectively) – which is also involved in offensive cyber operations.

B. ROLES AND RESPONSIBILITIES

Experts agreed that all persons conducting cyber operations remain subject to the applicable international and domestic legal frameworks. Although the blurring of civilian and military functions may make the determination of the relevant framework more difficult, no individual, State organ or other entity is outside the law. In this connection, some experts noted that the divide between military and non-military cyber operations by States often runs along similar lines as the divide between effects operations (i.e. operations designed to disrupt, deny or destroy target devices, systems or networks) and intelligence activities, and that in many States these are subject to different domestic legal frameworks and authorities.[18] It was also suggested that, to the extent possible, military actors should not engage in defending civilian networks and data against hostile cyber operations outside of armed conflict.

Some experts expressed concerns that while armed forces may be familiar with the requirements of IHL, this may not be the case for intelligence agencies operating in cyberspace. Further, one expert questioned whether some States might deliberately shift operations between agencies with a view to avoiding these obligations. This raises the question of how operations transition from collecting intelligence to delivering effects given these concerns and the fact that the international legal framework governing effects operations is much more developed than the framework governing intelligence operations. Experts emphasized that as soon as effects were under consideration, targeting methodologies and safeguards developed for military operations should be employed. One expert further noted that, in their experience, if an operation was to move from intelligence collection to the delivery of effects, then the original cyber tools and infrastructure used to conduct intelligence collection would normally be withdrawn and new or different cyber tools and infrastructure deployed. While this transition would be linked to a change in authorities and targeting methodologies, the primary reason was to preserve intelligence collection capabilities for future use.

When considering targeting processes and the associated authorities, the need was underscored to continuously adapt existing processes or develop new ones to ensure that military cyber operations were conducted with the same degree of assurance as conventional military operations. The limited amount of experience with these operations to date meant that politicians and policymakers often lack the necessary understanding to be able to make effective decisions to guide, supervise or approve military cyber operations. There was therefore a need for a programme of education, training and exercises in this respect. Finally, the importance of determining accountability for any violations that may occur in the context of military cyber operations was underlined.

Overall, discussing the role of the armed forces in the conduct of cyber operations remains challenging as the technical aspects of the operations are surrounded by secrecy and uncertainty, which results in very little informed public discussion. There was consensus that this lack of transparency contributed to the potential for misunderstandings and hence escalation. By contrast, transparency is closely linked to ensuring deterrence: it is very hard to deter one's adversaries without being open, at least to an extent, about one's capabilities, intent and aims. The lack of transparency was further reflected in the 'blurring' of the roles of different government agencies beyond the armed forces in the conduct of offensive cyber operations.

[18] For example, in the United States these are referred to as respectively as Title 10 and Title 50 authorities. See for example R. Chesney, "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries", *Lawfare*, 12 April 2018; A. E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action", *Harvard National Security Journal*, Vol. 3, 2011, pp. 85–142.

C. GREY ZONES

The challenge posed by the blurring of military and civilian roles in cyberspace led to a discussion concerning a so-called 'grey zone' between peace and armed conflict. Experts noted that in both academic and more general literature, this terminology had largely been used to describe how actors may be using hostile cyber (or other) operations in a harmful manner yet designed to avoid eliciting a conventional military response by the target, including through blurring the identification by the target of the applicable legal framework.

Some experts felt that it might be difficult to decide whether a cyber operation needed to be conducted under military or civilian authorities in these grey zones, in particular when a target of a grey-zone operation was considering what operation it might carry out in response. In addition, understanding and countering grey-zone operations is further complicated by the proliferation of proxies and other non-State actors utilized by some States to avoid attribution.

While the authorities and processes for conducting cyber operations were reasonably clear in peacetime and during armed conflict, it was suggested that there might be different understandings between States as to when they were in a situation of armed conflict. Some experts shared their experience that where there was any doubt, certain States applied the principles of IHL even if the context did not reach a level that might be legally defined as armed conflict.[19] One expert highlighted the Israeli 'Campaign Between Wars' concept as a relevant effort by a State to systemically deal with the 'grey-zone challenge', as well as to frame it and conduct orderly processes within it.[20]

KEY TAKEAWAYS

- States should continuously adapt existing processes or develop new ones to ensure that military cyber operations are conducted with the same degree of assurance as conventional military operations. This should involve the development of programmes of education, training and exercises for these purposes.
- States should avoid the blurring of the functions of the organizations involved in the conduct of State-run cyber operations so as not to jeopardize the protections afforded to civilian entities during armed conflicts.
- States should ensure that all organizations involved in the conduct of military cyber operations during armed conflicts, including but not limited to the armed forces and intelligence agencies, are acquainted with the scope of application, and requirements, of IHL.
- States should ensure that military cyber operations remain under the oversight and control of the appropriate authorities, and that there is accountability for any violations that may occur in the context of military cyber operations.
- States should strive to be as transparent and open as possible to informed public discussion with respect to the role of their armed forces in the conduct of cyber operations.

[19] See, for example, US Department of Defense, *Directive No. 2311.01E*, 9 May 2006, para. 4.1 ("Members of the DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and *in all other military operations*.") (emphasis added).

[20] For an explanation of this strategy, see G. Eisenkot and G. Siboni, "The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran's Malign Regional Influence", *The Washington Institute*, 4 September 2019.

3. MILITARY CYBER OPERATIONS

This chapter examines the meaning of the notion of military cyber operations, the way in which these operations are conducted during armed conflicts and the processes involved in developing military cyber capabilities. It explores whether it is possible – or useful – to clearly delineate offensive from defensive cyber operations, especially from the perspective of reducing the attendant risk of civilian harm. It then examines the utility of the alternative 'full spectrum' approach covering all military cyber operations during armed conflicts in order to direct and manage them and improve compliance with the law. Finally, it considers the risk of civilian harm linked to the development of cyber capabilities, and particularly to the potential availability of vulnerabilities and tools on the internet.

A. TYPOLOGY OF MILITARY CYBER OPERATIONS

Military cyber operations during armed conflicts can have a variety of potential aims and effects. Practically speaking – and putting aside the question of the conformity of such operations with IHL – this spectrum ranges from the strategic level, such as disrupting a country's economy or undermining its will to fight, through to more tactical or battlefield activities such as disrupting command and control or weapons platforms. Some experts also emphasized the potential significance of psychological effects on adversary armed forces, such as influence or deception.

With respect to the terminology used to describe such operations, experts noted that a number of different activities in cyberspace are labelled 'cyber attacks', which causes difficulties in developing shared understandings of risks and mitigations. These activities ranged from (1) the general probing for vulnerabilities, which is happening continuously, through (2) the positioning of malware for intelligence collection, signalling, coercion and/or deterrence, to (3) pre-positioning of malware for later disruptive purposes, including for physical effect. All experts agreed that a common lexicon remains an issue in advancing the discussion towards developing a shared and sufficiently nuanced understanding of risks to civilians.

Experts agreed that military cyber operations may be roughly categorized into exploitation, defence and offence:

- *Exploitation* is the accessing of adversary networks for the purposes of gathering information and intelligence.
- *Defensive cyber operations* are primarily about ensuring the security of a State's own networks; in a number of States, the role of the armed forces extends to contributing to defending wider critical infrastructure.
- *Offensive cyber operations* seek to project power against an adversary by disrupting, degrading or destroying their networks or other capabilities, including through the use of malware and by directly accessing and controlling enemy systems or networks.

However, the precise contours of each of these definitions are difficult to draw. In particular, several experts suggested that States may intentionally define offensive operations broadly in order to retain a wide discretion as to their response to malicious activities by others. For example, France distinguishes between 'offensive cyber operations' (*les opérations de la lutte informatique offensive*), which is a term with a broad meaning that includes efforts to influence perception and to interfere with the ability to analyse data,[21] and 'cyber attacks' (*les cyberattaques*), which cover only those operations that target equipment and systems such that these can no longer provide the service they were set up for, whether permanently or temporarily.[22]

[21] France, Ministère des Armées, *Éléments Publics de Doctrine Militaire de Lutte Informatique Offensive*, 2019, p. 6.

[22] France, Ministère des Armées, *International Law Applied to Operations in Cyberspace*, 2019, p. 13.

One of the challenges with these distinctions is that they may place undue emphasis on the supposedly ‘offensive’ purpose of military cyber operations. However, a State may also attempt to recover or delete its own data which had been stolen by an adversary. Even if such an operation was described as a ‘defensive cyber attack’, it could still constitute a risk of civilian harm through unintended damage to or loss of data other than that targeted. It was noted in this respect that IHL rules regulating attacks apply regardless of whether the attack is carried out in offence or in defence.[23] In the discussions at the meeting, ‘military cyber operations’ was thus used as a general term that encompasses operations conducted for both offensive and defensive purposes.

B. CONDUCT OF MILITARY CYBER OPERATIONS

Some experts drew on their operational background to argue that the divide between offensive and defensive military cyber operations, while reflecting traditional military doctrinal constructs, was not helpful in directing and managing military cyber operations. Rather, they suggested that what was needed was a ‘full spectrum’ approach, i.e. one that integrated all of the activities conducted by the armed forces in and through cyberspace, from building and securing networks, to disrupting adversary activities in times of armed conflict. These experts considered that such a broad understanding would help subject all military cyber operations during armed conflicts to the regulatory framework of IHL and thus improve compliance with the law and the avoidance of civilian harm. Other experts noted that cyber operations conducted by government agencies other than the armed forces already were, in most States, under legal controls and limits at least equivalent to those of IHL, but also incorporating domestic approaches to the respect of international human rights law. With respect to IHL specifically, experts underscored that States should make public their views concerning how this body of law applies to military cyber operations during armed conflicts.

The discussion then turned to the practical conduct of military cyber operations for effect, as framed by the ‘cyber kill chain’ and military targeting processes.[24] Although this is not a simple linear process, it is possible to distinguish between a phase during which the operators seek to gain access to the targeted element of the adversary network, and – if this is the aim of the operation - a phase during which the destructive or disruptive activity is initiated. One expert argued that during the initial access phase, en route to the target, there was low risk of civilian harm as operators were only seeking to develop their understanding of the network and how to move through it. As such, they were not likely to be deleting or modifying data in ways that risked unintended effects, and on the contrary would try to avoid doing so to remain undetected.

Lastly, experts emphasized the potential for military cyber operations to be less destructive and even less disruptive than conventional kinetic attacks. Not only could the damage inflicted on a target system be reversible if so desired and the operation has been appropriately designed to that effect, it could potentially even have an in-built time limit that returned the system to its normal operating condition. However, one of the challenges for such operations is being able to understand the extent of the interconnectedness and the system dependencies.

[23] According to Art. 49(1) of the 1977 First Additional Protocol, “‘[a]ttacks’ means acts of violence against the adversary, whether in offence or in defence”.

[24] For further discussion of targeting processes, including the concept of ‘cyber kill chain’, see Section III of the background document in Annex 1.

C. DEVELOPMENT OF MILITARY CYBER CAPABILITIES

The importance and the challenge of ensuring target discrimination when developing capabilities were underscored. Experts suggested that States with appropriate processes and control mechanisms in place would not employ indiscriminate capabilities with respect to which it is not possible to anticipate and control their spread. While bespoke tools can be developed, these are expensive, and their development is risky as the entire investment could be compromised by a simple patch. Therefore, one expert suggested that these tools were being developed only where the State felt that the gain was truly worth the effort and that the risk of the new tool being disabled by updates and patches was relatively low.

Experts also noted the extent to which vulnerabilities and tools were available openly on the internet, often as part of cyber security practices, to anyone who wished to take malicious advantage. Two projects maintained by the information security company Offensive Security were mentioned, the *Exploit Database*[25] and *Kali Linux*.[26] It was argued that the malicious exploitation of such publicly available resources posed a risk of civilian harm comparable to that caused by military cyber operations, but possibly without any legal and/or political oversight.

KEY TAKEAWAYS

- States should work towards a common lexicon concerning military cyber operations in order to advance the discussion on the risks that such operations pose to civilians, by developing shared and sufficiently nuanced understandings of these risks.
- States should be clear and public on their interpretation of how IHL applies to military operations in cyberspace.
- States should put appropriate processes and control mechanisms in place so as to prevent the employment of indiscriminate capabilities the spread of which would not be possible to anticipate or control.
- While military cyber operations may have the potential to be less destructive than conventional kinetic attacks, the armed forces should always understand the extent of interconnectedness and system dependencies before deciding to launch a cyber operation in specific operational circumstances.
- States should consider taking measures to address the availability of vulnerabilities and cyber tools on the internet and to prevent their exploitation by malicious actors.

[25] Offensive Security, Exploit Database.
[26] Offensive Security, Kali Linux.

4. ASSESSING THE RISK OF CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

The aim of this chapter is to contribute towards building shared understandings of the risk of civilian harm from military cyber operations during armed conflicts. It focuses on how the risk of civilian harm can and should be assessed during military cyber operations by actors seeking to ensure such operations comply with IHL. The chapter considers this question in two steps: firstly, how the risk of civilian harm might be *understood* in the context of a military cyber operation, including in the digital and cognitive domains; secondly, how this risk could be *assessed* during the conduct of such operations. The chapter concludes with a box on the practical application of the approaches identified during the discussion in relation to a set of hypothetical scenarios.

A. UNDERSTANDING THE RISK OF CIVILIAN HARM

Experts noted that collateral damage assessment methodologies developed for traditional kinetic operations tend to focus on two dimensions of risk: *quantitative* (i.e. the extent of damage or the number of civilians affected), and *qualitative* (i.e. the nature and severity of the risk). It was argued that understanding the risk posed by military cyber operations in both of these dimensions was potentially more complex than in the context of kinetic operations. The number of civilians potentially harmed could be enormous given global interconnectedness and the number of users, systems and network components that might be affected. The quality of civilian harm in some cases might be similar to those of kinetic operations if the cyber operation leads to physical damage, although the loss of data confidentiality, data integrity and data availability may also cause harm. These may in turn impact on the ability to use a network or system and its associated data, and therefore it is necessary to consider the extent to which that system is essential to civilian life.

While these risks are largely linked to the targeted system or network, including their dependencies and connection with other systems or networks, the nature of cyber capabilities themselves also entails risks. In particular, experts were concerned about ensuring that the risk that a tool might spread was controlled. It was argued that even though Stuxnet had targeted an air-gapped system, the malware spread globally (albeit with little to no significant impact as a result of its design).[27] Another capability-related risk that experts highlighted was that of reverse engineering, with the tool then being used to cause civilian harm unintended by the original designers.[28] Experts underscored that States should have mitigation strategies in place for all military cyber capabilities that they would consider developing, in order to minimize these risks.

The meeting also considered the difference between the nature of civilian harm caused by cyber operations and that caused by kinetic operations. Two key aspects were highlighted in this connection. Firstly, the type and extent of damage are significantly different. For instance, a cyber operation disabling the infrastructure of a previously well-functioning hostile online group may successfully cripple its activities, but only occasion a miniscule amount of quantifiable physical damage. Secondly, cyber operations may also be different in terms of their temporal characteristics, with the effects caused by such operations being potentially

[27] For further discussion of Stuxnet, see Section IV of the background document in Annex 1.

[28] See for example Kacy Zurkus, "Stuxnet Returns, Striking Iran with New Variant", *InfoSecurity*, 2 November 2018, where it is reported that over 22 million pieces of malware have used the Stuxnet "attack blueprint" to attack States and organizations around the world.

temporary whereas physical damage can take a long time to repair. Conversely, cyber and kinetic operations can both cause long-terms effects albeit significantly different in their nature: for example, the deletion of essential civilian datasets may bring about lingering long-term civilian harm that will vastly exceed the moment when the operation in question was launched, while bombs can cause lifelong disabilities.

The responsibility of States to understand the critical connections and dependencies in their own networks was also underscored. While this issue is not directly related to the targeting of military cyber operations, it was argued that because States have primary responsibility for the safety and security of their citizens, they should have sufficient understanding to be able to focus defensive efforts at the key nodes and also to be able to restore their functionality in the event of a destructive or disruptive attack. This would also be part of their obligation to protect civilians and civilian objects under their control from the effects of attacks during armed conflict.[29] Doing so is essential in order to prevent the 'domino effect' that adversaries' offensive operations may otherwise cause.

B. ASSESSING THE RISK OF CIVILIAN HARM

Experts were in agreement that, in order to assess the risk of civilian harm from military cyber operations, existing processes developed for the purposes of kinetic operations should be used as a general frame of reference and adapted to account for the new challenges posed by cyber operations. Armed forces have been conducting assessments of the risk of civilian harm from their activities for some time and there are well-established methodologies in place, normally labelled collateral damage estimation (CDE) processes.[30] These make up a part of broader targeting processes that seek to ensure that armed forces are both efficient in their use of weapons and compliant with the requirements of international law, particularly IHL.

One expert suggested that kinetic targeting CDE processes considered relatively closed and static systems, whereas military cyber targeting had to engage with more complex and dynamic ones. This complexity arises from the interconnected and interdependent nature of many networks and systems, which means that effects can sometimes occur at considerable distance from the targeted system. Another expert highlighted the need to also consider the spread of corrupted data as systems share information. The need to consider broader and longer-term impacts was underscored as well, such as a loss of trust in critical information systems by the population that may result from a cyber operation.

Experts highlighted the need for targeting processes to not only consider the technical challenges but also those associated with the human dimensions of cyber security such as system administrators and cyber security teams. Operators should also take into account that an action taken in response to an otherwise precisely targeted cyber operation may inadvertently cause a greater impact and hence risk civilian harm in a way that the original operation had not intended. For example, an actor conducting an attack on a military facility might seek to disrupt the power supply to that facility. In doing so, it accesses a local power grid; but the CERT, seeing this, believes it to be part of an attack on that grid. The CERT thus shuts down the power grid to manage the perceived threat, which in turn cuts off the electricity supply to the military facility as well as the civilian population.

Complex assessments that have to be made during the targeting process may well require a considerable investment of resources. This may include the potential building of facilities where models of targeted systems could be used as part of assessment processes (so-called 'cyber ranges'). These may be used together with advanced AI capabilities that can simulate the real 'internet', or at least large and complex sets of integrated environments and networks. While experience with military cyber operations was also key to ensuring effective analysis of the risks, one expert additionally noted the potential to use scenario-based approaches where systems had failed as a result of natural disasters or other forms of human action. Such case studies

[29] See Article 58(c) of the 1977 First Additional Protocol; ICRC Customary IHL Study, Rule 22. See also the discussion of precautions against the effects of attacks in Section 5.C below.

[30] For further discussion of processes for assessing the risk of civilian harm, see Section V of the background document in Annex 1.

might provide useful insights into the extent of harm that may be anticipated as a result of cyber operations targeting those or similar systems.

It was noted that the resource-intensiveness of some of these assessments might exclude smaller or less cyber-developed States from being able to conduct some of the more complex offensive military cyber operations. Nonetheless, experts agreed that, like for any other military capability or operation, the lack of available resources is not a valid justification for conducting cyber operations without making careful risk assessments.

Beyond the complexity of the analysis, experts also noted its dynamic nature. Any assessment is time-bound and requires a continuous dynamic assessment approach. In some cases, this might be achieved through the network access allowing ongoing assessment and the tool itself being developed and adjusted as operators learn more about a system and respond to ongoing changes in it.

While there was not universal agreement as to a finite range of additional questions that needed to be considered over and above traditional CDE processes, suggestions included:

- Is this operation using a vulnerability that is widespread? In this respect, one expert highlighted the Shodan search engine as a useful tool for identifying the spread of vulnerabilities in internet-connected systems.[31]
- How easy will it be for the targeted system to be reconstructed?
- Does the operator understand how the capability will affect networks connected to the target system?
- What are the risks arising from the interaction between the target systems' cyber defences and the cyber capability used?
- Has the operator taken action to protect its own systems against the capability and (where appropriate) informed third parties of the risk?
- Does the operator understand whether the capability can be re-engineered and used against the actor or a third party, and what is the potential risk of civilian harm in such case?

In closing, experts highlighted that such analysis requires expertise from a wide range of sources which, in turn, needs to be put into straightforward language for decision makers who might be less familiar with military cyber operations and the risk of civilian harm they entail.

[31] See Shodan.

PRACTICAL APPLICATION

During the meeting, experts discussed a series of scenarios set in a fictitious armed conflict to focus on practical aspects of the assessment and mitigation of the risk of civilian harm from military cyber operations in armed conflicts. These scenarios included the potential use of military cyber operations against a dual-use port facility, a sensitive manufacturing site, the fuel supply for an elite military unit, the servers involved in a command and control facility, and a local electricity power grid (see ***Annex 2****). This box highlights the key insights from the discussion related to understanding and evaluating the risk of civilian harm from military cyber operations.*

Avoiding or at least minimizing incidental civilian harm is a legal obligation during armed conflicts, and all experts agreed that it must be standard operating practice for any actor in a conflict situation. In discussing the scenarios, experts proposed various key considerations by way of generalization from existing operational planning approaches:

- One expert proposed to divide the questions to be asked into three categories: (1) *strategic* (what problem have we identified and how do we propose to address it?), (2) *operational* (what effect do we wish to gain and what options are there to achieve it?), and (3) *tactical* (what specific operation and when exactly should it be carried out?).[32]
- Another expert proposed the 'centre of gravity approach', which entails three criteria: (1) *criticality of the target* (is this a critical target?), (2) *likelihood of success* (how likely is it that the operation will hit the target?), and (3) *unintended consequences* (what civilian harm is the operation expected to cause and what mitigations can be used?).
- Adopting a more detailed lens, yet another expert explained that any operational planning should consider the (1) *extent and duration of the expected effect*, (2) *type and age of the targeted technology*, and (3) *number of persons (both military and civilian) affected by the operation*.

All of the scenarios involved networks, systems or facilities used for both civilian and military purposes. Several experts noted that this dual-use character of potential targets highlighted the necessity for military cyber operators to be scrupulous in applying the relevant IHL principles. This was not limited to the immediate target system but also to its role in broader systems or networks and the risks of indirect effects also in these broader interconnected systems or networks. For example, in considering a cyber operation that would disrupt military logistics going through a port by corrupting the shipping data (**Scenario 1**), experts highlighted the risk that containers carrying dangerous goods may be inadvertently mishandled, resulting in explosions or the release of hazardous materials. Further, other experts highlighted the importance of understanding the port's role in the State's broader economic system and the extent of civilian harm that would be caused through the 'ripple effect' of the port disruption or possibly even the shutdown incidentally caused by targeting its military logistic function. It was noted that from an operational perspective, the commander would consider whether the intended effect could be achieved by targeting a different, non-dual-use facility, instead of the port. Doing so is also a legal requirement under IHL, which mandates that when a choice is possible between several military objectives for obtaining a similar military advantage, the commander must choose that objective the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.[33]

[32] It should be noted here that the strategic/operational/tactical construct does not equate to the levels of conflict but rather the expert's framework for focusing a problem.

[33] See Art. 57(3) AP I; ICRC Customary IHL Study, Rule 21; see also ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts – ICRC position paper', November 2019, p. 6 ("during military operations, including when using cyber means or methods of warfare, constant care must be taken to spare the civilian population and civilian objects; all feasible precautions must be taken to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare").

Some experts highlighted the need to understand the general conditions that the civilian population is facing. For example, if the electricity grid in the target country suffered from frequent blackouts, a military cyber operation that caused an additional two-hour shutdown (as proposed during the discussion of **Scenario 5**) would have to consider this general situation. In this case, it would also be necessary to assess whether specific facilities such as hospitals and other critical infrastructure had appropriate back-ups and whether other factors such as the weather could contribute to increased civilian harm. However, some experts also highlighted the challenge of understanding all of the potential network effects, citing the example of the 2003 power blackout throughout parts of the United States and Canada, during which an apparently minor failure in one small part of the network had cascading effects that impacted on the power supply to some 50 million people.[34] It was also noted that the impact on civilians affected by such disruptive cyber operations goes beyond the immediate harm and includes various long-term psychological/cognitive effects such as the decrease in trust in the cyber domain or even in the government among the affected populations.

Several experts emphasized that cyber operations form only some of the tools that are available to a military commander. For example, in a scenario concerning a possible military operation against a fuel supply relied on by the adversary's mobile elite unit (**Scenario 3**), it was noted that the objective of the operation could be achieved by non-cyber means, including a kinetic strike against the fuel supply or an attack against the unit's communications systems instead of the fuel station. As above, if these options are feasible and offer the prospects of obtaining a similar military advantage, the commander must select the one (whether cyber or non-cyber) that is expected to cause the least danger to civilian lives and civilian objects.[35]

The scenarios reflected that individual States may have varying cyber capabilities at their disposal. Specifically, one of the belligerents was described as possessing significantly more advanced offensive cyber capabilities than the other. In that regard, some experts were of the view that it would in any case be unrealistic to expect 100% mission assurance, especially for States with less advanced cyber capabilities. Others noted that the logic of IHL rules mandating 'all feasible' precautions implies that States with more capabilities would be required to do more than those that are less advanced.

Finally, it was noted by some experts that for many dual-use facilities (such as the port facility discussed in one of the scenarios) there was a degree of international standardization and therefore information available to assist military cyber operators with assessing the risk of civilian harm. This includes information on networked industrial control systems which would be the potential vectors for military cyber operations to deliver the desired effects in some of the scenarios.

[34] See also US-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004.

[35] See note 33 above.

KEY TAKEAWAYS

- States should have mitigation strategies in place for all military cyber capabilities that they consider developing in order to minimize the risk of civilian harm associated with the deployment of such capabilities.
- In the planning and conduct of military cyber operations, States should involve expertise from a wide range of sources which, in turn, should be put into straightforward language for decision makers who might be less familiar with military cyber operations and the risk of civilian harm these operations entail.
- To assess the risk of civilian harm from military cyber operations, existing processes developed for the purposes of kinetic operations should be used as a general frame of reference and adapted to account for the new challenges posed by cyber operations.
- In addition to collateral damage estimation and other traditional processes, States should consider additional cyber-specific questions such as those listed on p. 21 of the present report and develop relevant processes accordingly.
- Notwithstanding the possible resource-intensiveness of doing so, States must always make careful risk assessments before conducting cyber operations in specific circumstances.
- In planning and conducting targeted cyber operations, States should take into account that the remedial action by the target may inadvertently cause a greater impact and hence risk civilian harm in a way that the original operation had not intended.
- States should have a sufficient understanding of the critical connections and dependencies in their own networks in order to be able to focus defensive efforts at the key nodes and to restore their functionality in the event of a destructive or disruptive attack.

5. MEASURES TO AVOID OR REDUCE CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS

This chapter considers measures that could be taken to mitigate the risk of civilian harm from military operations during armed conflicts. It begins by discussing the balance of responsibility between those conducting offensive military cyber operations and those defending networks in avoiding or reducing the risk of civilian harm from military cyber operations. It also explores which practical and technical mitigations could be used by both attackers and defenders. The chapter then considers legal and policy preventive measures that can be adopted in order to avoid or reduce the risk of civilian harm. Like the previous chapter, it ends with key insights from the experts' discussion about the practical application of these measures in a range of hypothetical scenarios.

A. OWNERSHIP OF RISK – ATTACKERS AND DEFENDERS

There was general agreement among experts that in order to avoid or at least reduce the risk of civilian harm from military cyber operations, there was a responsibility on those taking offensive action and on those whose networks and systems were at risk of being attacked. This duality of responsibility is also reflected in the norms of responsible State behaviour in cyberspace adopted by the UN.[36] Specifically, one of the norms mandates that States should not conduct cyber operations that would damage critical infrastructure,[37] while another one provides that States should take appropriate measures to protect their own critical infrastructure.[38] This dual responsibility is also reflected in IHL through the obligation to take precautions in attack and precautions against the effects of attack.[39]

All experts agreed that States had a responsibility to reduce the risk of civilian harm through appropriate cyber security measures, including both practical measures and ensuring public awareness. Experts highlighted the potential role for international organizations in setting standards for cyber security in their sectors. For instance, the International Maritime Organization had developed such standards for commercial shipping,[40] and the International Atomic Energy Authority provides guidance for the nuclear power sector.[41] One expert noted that in terms of the protection of critical infrastructure, information security governance frameworks

[36] See United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, pp. 7–8 para. 13. The report was later endorsed by a unanimously adopted resolution of the UN General Assembly. See UN General Assembly, Resolution 70/237, *Developments in the field of information and telecommunications in the context of international security*, adopted on 23 December 2015.

[37] *Ibid.*, p. 8 para. 13(f).

[38] *Ibid.*, p. 8 para. 13(g).

[39] See Arts 57 and 58 of the 1977 First Additional Protocol, and Rules 15-21 and 22-24 of the ICRC Customary IHL Study.

[40] See International Maritime Organization, Maritime Cyber Risk.

[41] See International Atomic Energy Agency, Computer and Information Security.

provide accessible and adaptable international benchmarks and platforms for both well-resourced and under-resourced States and utilities to achieve cyber resilience and mitigate civilian risk.[42]

However, several experts cautioned against placing ownership of the risk on the defender and, more specifically, against 'victim blaming'. In their view, it is inappropriate and counter-productive to hold the defender responsible for the risks created by an attack on its network and systems. Placing the blame on the defender for failing to patch its systems sends "the wrong message" and may be discouraging in the long term. Blaming the victim is not an effective strategy in criminal law and should be avoided in the cyber security field too. Instead, one of these experts suggested that the focus should move from victims to 'enablers', such as certain domain registrars whose recklessness – for example, by allowing malicious actors to register a domain under false pretences – facilitates much of the malicious activity online.

Experts agreed that reducing and mitigating risks created by both offensive and defensive cyber operations involved the interplay of three factors: means, behaviours and processes. While the lack of means such as economic resources and technical aptitude may pose challenges especially for some smaller States, experts noted that all States could and should ensure that they adopted the appropriate behaviours and employed rigorous decision-making processes when it came to conducting military cyber operations.

B. PRECAUTIONS IN ATTACK

Experts then turned to potential technical measures that could be taken to avoid or at least reduce incidental civilian harm during offensive cyber operations. At the outset, several experts cautioned that not all offensive military cyber operations involve the deployment of malware. In their view, it would thus be too reductionist to focus the debate only on technical measures that could or should be built into bespoke malware capabilities (i.e. 'cyber weapons'). In some operations, the attacker may simply aim to gain access to a system or network and/or obtain system administrator privileges without necessarily using any malware to subsequently create an effect. In such cases, the offensive operation consists of taking direct control of the target system and attached devices in order to achieve desired effects. An example of this sort of operation was the interference with the electrical grid in Ukraine in 2015.[43] Accordingly, in such operations, mitigation is not so much a question of building in technical measures, but rather a matter of appropriate decision-making processes and considerations to be taken into account once access and control have been secured.

Returning to operations that do involve the deployment of malware to create the desired effect, experts suggested a number of technical approaches that could contribute to reducing the risk of civilian harm. In particular, experts highlighted smart malware capable of 'system-fencing', i.e. the ability to recognize the environment it finds itself in and then execute itself only if the target system precisely matches that environment. It was suggested that Stuxnet was an illustrative example of this approach, because it was designed to only operate in a system with a specific configuration of Siemens programmable controllers.[44] Among other feasible mitigation methods, 'geo-fencing' is a technique that limits the malware to only operate in a specific IP range, and a 'kill switch' is a technical feature that disables the malware after a specified time period or when remotely activated. Moreover, one expert noted the possibility that malware can contain an autodelete feature, whereby it wipes itself off the target system once it achieves its goal. However, that expert also warned that such a functionality may be inappropriate in more sophisticated cyber tools given the risk that it may malfunction and thus unintentionally corrupt the entire target system or network. Depending on the situation, a combination of several of these risk-mitigation functionalities could be used for the same malware to minimize the risk as much as possible.

[42] See for example US National Institute of Standards and Technology (NIST) Cybersecurity Framework; ISO 27001/2; Information Technology Infrastructure Library (ITIL); and Control Objectives for Information and related Technology (COBIT).

[43] For an analysis of this operation, see K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, 3 March 2016.

[44] For further discussion of Stuxnet, see Section IV of the background document in Annex 1.

Some experts suggested that potentially the most reliable way of ensuring that an offensive cyber tool did not cause unexpected effects and civilian harm was to keep it under direct command and control through all phases of the operation. They admitted that continuous command and control also increased the risk of the operation being detected and attributed but noted that such a risk was likely to be considered less significant during periods of armed conflict. It was suggested that the correct approach to mitigation was one of direct proportion between autonomy and safeguards: the more autonomous a particular tool is, the stronger in-built safeguards it should have (such as suspending its operation or switching itself off when certain conditions are met).

Experts also discussed the risk of reverse engineering of offensive cyber capabilities and 'blowback' where a tool is targeted back against the originating State or against a target other than the one it was originally designed to be used against. While encryption is one way to mitigate the risk of reverse engineering, it was also suggested that States might want to submit their malware once it had been used to a site such as VirusTotal.[45] This would ensure that the international cyber security community became aware of the signature and that it was then included in anti-malware package updates relatively quickly, thus reducing the risk of its reuse by third parties. However, if, for example, the original tool had been set up with geo-fencing, this could be removed through reverse engineering and then the malware might not be detected by the anti-malware software. Furthermore, an expert noted that one obvious downside of declaring one's used cyber capability publicly was that the State would not be able to use that capability again.

C. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

As noted earlier, while the experts were generally concerned about the risk of 'victim blaming', they agreed on the importance that States nonetheless contribute to reducing the risk of civilian harm by taking cyber defence measures. They agreed that all States should be building strong cyber resilience cultures across society by increasing public awareness of the risks and engaging with the private sector, which owns the relevant infrastructure in most cases. This would mitigate the risks caused by any cyber attack, whether military cyber operations, criminal cyber operation or other.

Experts also highlighted the risk created by the dual-use character of much of the cyber infrastructure, meaning that it is shared by both civilian and military users. Some experts also expressed concern that some less responsible actors could deliberately choose to host essential military systems amongst civilian data to try to shield such systems from hostile military cyber operations by increasing the risk for the attacker to cause incidental civilian harm. While all experts agreed that such practices had to be actively discouraged, it was also noted that financial pressures were leading to more military data being hosted on commercial cloud services.

However, a contrasting trend was also noted. In some cases, military cyber infrastructure, including military networks, is relatively disconnected from the internet for its own defence, i.e. to minimize its attack surface. Once an adversary succeeds in penetrating such military network of the enemy and spreads a destructive malware there, the network's disconnection 'frames' the attack, and thus serves to protect the outside civilian networks and infrastructure. Nonetheless, it was noted that even in such cases, civilian cyber infrastructure may still be affected if it is used as a penetration channel en route to the target system, even if the attendant risk of civilian harm was low.[46]

The discussion then turned to the possibility of digitally marking protected objects as a possible passive precaution. Experts noted that to do so was technically possible, for instance with Internet Protocol version 6 (IPv6), which allows for designating specific IP address blocks as protected. However, others expressed

[45] VirusTotal.

[46] See the discussion in Section 3.B above (p. 17).

scepticism as to the effectiveness of this practice in deterring malicious activity. In particular, it was highlighted that criminal organizations are already targeting hospitals for financial gain and digital marking would only make this easier. Some experts also cautioned that such a system could be misused to protect military critical systems despite the fact that doing so would be as impermissible as painting a red cross on the roof of military barracks. However, overall there was agreement that digital markings could be considered a way to potentially reduce the risk of incidental civilian harm caused through military cyber operations.

The UN norms of responsible behaviour also mandate that States should not deliberately harm the computer emergency response teams (CERTs) of other States.[47] In that connection, experts discussed the need to protect 'first responders' in cyberspace similarly to medics providing first aid in the physical world. Several experts considered that analogies were difficult to make in this context. Specifically, cyber first responders differ significantly from medics, firefighters or civil defence organizations, given that the role of the former is not just to provide the equivalent of first aid, but typically also to identify the source of the attack and bring the attack to an end. While the experts did not reach an agreed conclusion, it was generally accepted that the nature of cyberspace meant that direct comparison with the physical domain was challenging in this context.

Lastly, experts emphasized the importance of attribution in holding actors to account when there has been civilian harm, which is a key factor in terms of ensuring compliance with the law and thus mitigating the risk of civilian harm. It was noted that although it had long been thought that attribution of cyber operations to States was almost impossible, this was no longer true. According to one expert, the key obstacle is not in attributing the attack, but rather in publishing the evidence of attribution; still, recent practice shows that if an attack crosses a certain threshold, the victim State will make a public attribution statement. In that expert's view, in deciding whether to conduct a hostile cyber operation, States now need to factor in the substantial chance that the operation will be attributed to them.

However, other experts argued that attribution by individual States had had limited effect and that new mechanisms for collective attribution had to be developed. Overall, it was recognized that to date this had proved difficult because, as noted, States were reluctant to expose the methods by which they had obtained the information necessary for attribution, and that the process of attribution was as political as much as technical. Private-sector cyber security companies may also play a role in this regard, with some of them possessing technical attribution capabilities that approach those of the most cyber-capable States. However, a few experts expressed concern that in some cases the link between certain private-sector organizations and States undermined the credibility of their attribution.

D. LEGAL AND POLICY PREVENTIVE MEASURES

Experts generally agreed on the importance of States continuing dialogues about norms of behaviour regarding military cyber operations whether through UN processes, other international forums or bilaterally. In this connection, one expert highlighted research conducted by the International Information Security Research Consortium on the implementation of norms, rules and principles of responsible behaviour by States with regards to information communication technologies. The final report makes specific recommendations on the possible progressive development of international law.[48] Other experts considered that international efforts should focus on the interpretation and application of existing international law in the cyber context rather than on the development of new law; in their view, cyber operations were not so special to prevent the application of existing law.

[47] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, p. 8, para. 13(k).

[48] A. A. Streltsov and E. Tikk (eds), *Methodological Issues of the Application of Norms, Rules and Principles of Responsible Behaviour of States to Promote an Open, Secure, Stable, Accessible and Peaceful ICT Environment*, International Information Security Research Consortium, 2020.

The discussion then turned to the role of IHL. All experts agreed that IHL restricted military cyber operations during armed conflicts. Some experts noted that while it was undoubtedly positive that many States committed themselves to its application, challenges remained as to the interpretation in the cyber context of key legal concepts such as the notion of ‘attack’ under IHL or ‘territory’ under general international law, including with respect to the role of territorial limits for the application of IHL or the law of neutrality, for instance.

Some experts also noted the need to continue to educate armed forces as to the implications of applying IHL to cyber operations. While most State armed forces understand the applicable legal constraints when using conventional weapons, in many cases there is less of a discussion about the employment of cyber capabilities and indeed how to assess and mitigate/reduce the risk of civilian harm when employing such capabilities. In part, this reflects the general levels of secrecy surrounding such operations.

Accordingly, some experts suggested that those States with the most experience should be prepared to share relevant information more publicly, including about how they had mitigated the risk of civilian harm in their actual operational practice. Others considered that the ICRC should also play a role in capacity building, as it does with respect to other aspects of application of IHL.

PRACTICAL APPLICATION

*During the meeting, experts discussed a series of scenarios set in a fictitious armed conflict to focus on practical aspects of the assessment and mitigation of the risk of civilian harm from military cyber operations in armed conflict. These scenarios included the potential use of military cyber operations against a dual-use port facility, a sensitive manufacturing site, the fuel supply for an elite military unit, the servers involved in a command and control facility, and a local electricity power grid (see **Annex 2**). This box highlights the key insights from the discussion on the forms of mitigation that might be utilized to ensure that any potential risk of civilian harm was avoided or at least minimized in the event that a military cyber operation was conducted.*

In considering most of the scenarios, experts discussed ways to ensure that the effects of the military cyber operation, both intended and unintended, would be reversible. There were a number of approaches discussed to achieve this, including the potential for a ransomware-style attack where the password would be released once the attacker had achieved the desired effect, thus reducing the risk of any further unintended civilian harm.

Experts agreed that one way of mitigating civilian harm is to carefully tailor the military cyber operations being planned. For example, in reference to the scenario involving the port facility mentioned earlier (**Scenario 1**), one expert noted that the attacker could avoid considerable harm to civilians by tailoring the operation to only corrupt the data related to specific terminals, ships or containers rather than putting a ransomware on the entire system, which would have the effect of shutting down the entire port. This way, the party to the conflict would limit the effect of its operation to causing disruption to the adversary's armed forces logistics capabilities while leaving civilian shipping unaffected.

In another scenario, which involved an air-gapped (i.e. physically isolated) target system and a risk of very serious unintended damage from the explosion of rocket fuel (**Scenario 2**), experts suggested that the only really effective way to minimize the risk of civilian harm was to ensure constant or at least regular direct control over any malware released into the system or indeed to deliver the effect through direct control. This would require either a human operator on the target system or the establishment of some form of remote access, and it was noted that this came with an associated risk to the successful conduct of the operation as any effort at direct control was vulnerable to detection.

Experts also emphasized that any efforts to minimize the risk of civilian harm were vulnerable to the unintended consequences of activity by the cyber defender. Thus, even direct control could be interrupted if the activity was spotted on the system or network with possibly unintended harmful consequences if the control aimed at ensuring the malware operated in a way that did not impact civilians. Similarly, controls such as kill switches built into malware had the potential to be accidentally disabled by defending operators.

Lastly, it was highlighted that cyber-enabled information operations could play a part in reducing civilian harm by messaging the population about attacks (whether cyber or kinetic) in order to allow the civilians to take appropriate protective measures. For example, one expert mentioned the Israeli practice of sending text messages to civilians in the Gaza Strip who are residing in or near buildings designated for imminent attack.[49] One of the scenarios involved a contemplated counteroffensive by armed forces on land (**Scenario 5**); experts noted that similar cyber operations (e.g. hacking the telephone network and sending a text message to everyone in a certain area) could be utilized to warn the civilian population to move out of the zone where hostilities will take place.

[49] L. Goldman, "IDF sends text message to Gaza mobile phones: 'The next phase is on the way'", +972 Magazine, 16 November 2012.

KEY TAKEAWAYS

- States should build strong cyber resilience cultures across their societies through increasing public awareness of the risks and by engaging with the private sector.
- States should not host essential military systems amongst civilian data to try to shield such systems from hostile military cyber operations.
- The idea of utilizing digital watermarks to identify protected facilities and networks akin to the Red Cross emblem should be explored further as a way of potentially reducing the risk of incidental civilian harm caused by military cyber operations.
- In the development of military cyber capabilities, States should utilize technical approaches that can contribute to reducing the risk of civilian harm, including 'system-fencing', 'geo-fencing', 'kill switches' and autodelete features (see p. 26 above for details). Depending on the situation, a combination of several of these functionalities may be used for the same malware to minimize risk as much as possible.
- States should continue to educate their armed forces as to the implications of applying IHL to cyber operations.
- States should develop and employ specific targeting processes for military cyber operations that ensure the application of the principles of IHL and that are integrated with other targeting processes.
- States and other stakeholders should work towards a better understanding of the opportunities that information operations offer to avoid civilian harm during armed conflicts and the risks they may pose.
- States should consider submitting their malware, once it has been used, to sites designed to aggregate and detect malicious content, in order to ensure that the international cyber security community becomes aware of the signature and that it is then included in anti-malware package updates, thus reducing the risk of its reuse by third parties.
- States with the most operational experience should share relevant information more publicly to the extent possible, including about how to mitigate the risk of civilian harm in actual operational practice.
- The ICRC should play a role in capacity building, similar to its activities with respect to other aspects of application of IHL.

6. FUTURE DEVELOPMENTS IN MILITARY CYBER OPERATIONS AND THEIR IMPACT ON THE RISK OF CIVILIAN HARM

The final chapter considers ways in which military cyber operations might develop in future and how this development might impact the risk of civilian harm. It first considers the implications of artificial intelligence, machine learning and autonomous weapon systems, before moving on to assess the impact of the Internet of Things and quantum computing. The chapter closes by discussing the relationship between military cyber operations and developments in the nature of warfare.

A. ARTIFICIAL INTELLIGENCE AND AUTONOMY

Overall, experts agreed that it was likely that artificial intelligence (AI) would play a significant part in military operations in cyberspace in the future. However, they also noted that it was extremely difficult to predict how this might influence such operations as there was so far little accumulated experience and few records of its use. Nonetheless, experts agreed that there was an ongoing competition among States for leadership in the development of AI, as evidenced by national strategies including those issued by China,[50] Russia[51] and the US.[52]

In the context of military cyber operations, experts noted that AI would be able to make a significant contribution to cyber defence through automating routine tasks such as scanning networks, patching vulnerabilities, and reviewing system logs. Indeed, several experts considered that in States where there was a shortage of cyber skills in the workforce, AI had the potential to allow a smaller pool of experts to be focused on the more specialist and less routine tasks. The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge had already demonstrated that AI-enabled systems could identify and patch vulnerabilities far faster than an experienced and highly capable human team.[53]

Experts also expressed concern about the risks associated with the employment of AI-enabled systems in military cyber operations. In particular, it was felt that AI is built around algorithms produced by humans and that it is therefore subject to errors and vulnerabilities, which may then be compounded, in the case of machine learning, by further AI-developed algorithms. One expert argued that if attackers have an understanding of how an AI-enabled system of an adversary operates and knowledge of its limitations, they may be able to target that system to subvert it and cause it to malfunction.

[50] China, State Council, *New Generation Artificial Intelligence Development Plan*, 20 July 2017 (English translation by Graham Webster *et al.*).

[51] Office of the President of the Russian Federation (2019), *Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation*, 10 October 2019 (English translation by CSET) (referring to risks associated with the wider development of AI, although not specifically focusing on military applications of AI).

[52] US Executive Office of the President, National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, Washington, DC, October 2016 (calling for the development of a government-wide and IHL-compliant policy on AI-enabled autonomous and semi-autonomous weapon systems).

[53] See D. Fraze, *Cyber Grand Challenge (CGC) (Archived)*, DARPA.

Experts also discussed the meaning of autonomy in the context of military offensive cyber operations. The definition used by the ICRC of an autonomous weapon system (AWS) is one that, once activated, selects and applies force to targets without human intervention.[54] Some existing military cyber capabilities could fit this description. Moreover, one expert suggested that there was a difference between, on the one hand, simple autonomous cyber capabilities, i.e. those not under full and direct human control but subject to specific programming and, on the other hand, AI-enabled autonomous cyber capabilities, which might more accurately be described as independent in their functioning.

Experts then discussed the potential for autonomous cyber systems, including those that are equipped with AI, to be used in a manner that would be more compliant with IHL than in situations where humans retain full control of the tools used. The general consensus was that the evidence for such a conclusion has not been established. One of the experts opined that given the risks involved in the deployment of autonomous systems, States would insist on maintaining a human decision maker in the loop for the foreseeable future. Similarly, it was argued that, in the conduct of hostilities, commanders or operators must retain a level of human control sufficient to allow them to make context-specific judgements to apply IHL.[55]

Finally, another expert recalled the framework of the 1980 Convention on Certain Conventional Weapons (CCW) and its role as a dedicated international platform for the discussion of issues related to emerging technologies in the area of AWS and noted its applicability to managing the development of autonomous cyber capabilities.[56] It was noted that the Group of Governmental Experts established by the 2016 CCW Review Conference affirmed in its 2017 report that (1) CCW offers an appropriate framework for dealing with the issue of emerging technologies in the area of AWS, (2) IHL applies fully to all weapon systems, including the potential development and use of AWS, and (3) States must ensure accountability for lethal action by any weapon system they use.[57] In the expert's view, the CCW framework provides a potentially effective way to manage the development of these capabilities and the attendant risk of civilian harm.

B. INTERNET OF THINGS AND QUANTUM COMPUTING

Experts were generally cautious about speculating how technological developments would impact on military cyber operations and the risk of civilian harm. However, it was noted that the expansion of the Internet of Things (IoT) was increasing the attack surface and the range of vulnerabilities available to be exploited by malicious actors. Several experts considered that this was already an existing concern and the 2016 Mirai Botnet incident was cited as an early example in this regard.[58] One expert highlighted that this distributed denial of service (DDoS) attack was targeted against key civilian providers of internet services, which contributed to the discussion on the changing nature of warfare outlined below.

Most experts felt that it was too early to identify the impact of developments of quantum computing. There was a shared understanding that quantum computing would dramatically increase computational power available, and hence the volume of data that networks would be able to handle and the speed at which it could be processed would likewise increase. It was also noted that quantum computing would have a significant impact on cryptography, which in turn could well impact on military cyber operations.

Likewise, it was suggested that blockchain would continue to contribute to improving cyber defence particularly through identity and supply chain management.

[54] ICRC, *ICRC Position on Autonomous Weapon Systems*, Geneva, 2021, p. 2.

[55] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting To Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, Geneva, 2019, p. 29.

[56] See also UN, *Background on Lethal Autonomous Weapons Systems in the CCW*.

[57] Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)*, CCW/GGE.1/2017/CRP.1, 20 November 2017, p. 4, para. 16(a)–(c).

[58] See "Inside the infamous Mirai IoT Botnet: A Retrospective Analysis", *The Cloudflare Blog*, 14 December 2017.

Overall however, experts generally agreed that while the development of technology had the potential to increase the risk of civilian harm through military operations in cyberspace, at the same time the capacity of States to understand those risks and mitigate them developed at a similar pace and should be fully used.

C. THE DEVELOPING NATURE OF MILITARY CYBER OPERATIONS

Finally, experts discussed several developments in terms of the nature of operations that were characteristic of military cyber operations, namely the role of non-State actors, the range of potential targets, and the recourse to hostile operations below the threshold of armed conflicts.

While the focus of the meeting was specifically on military cyber operations, governments and the armed forces do not have a monopoly on advanced cyber tools. One expert argued that cyberspace is "the only domain of warfare in which the armed forces of nation states do not dominate". It was highlighted in this regard that cybersecurity companies have the ability to analyse cyber attacks and attribute them in ways that had previously been limited to States. Moreover, some non-State actors have the potential to deliver effects through cyber tools comparable to or exceeding those available to many States. It was also highlighted that the availability of *Kali Linux*[59] since 2013 had further increased the range of tools available for malicious actors. Experts further noted that the role of non-State actors in the cyber domain is likely to continue growing in the future, thus creating a need – and opportunity - for public-private partnerships, but also that such forms of co-operation will further blur the line between military and civilian objects and persons.

With regard to the range of potential targets for malicious acts in and through cyberspace, some experts noted that the 'target space' was shifting away from traditional military targets, with States allegedly launching cyber operations against election infrastructure, domain name servers and cyber security companies. One expert noted that States are discovering that such operations offered effective (but less lethal and less escalatory) ways of imposing one's will on an adversary, which suggests that they will become a staple of 21st century statecraft, though this raises serious issues in terms of compliance with international law, including IHL.

These trends were also linked to the concern about the extent of malicious cyber operations taking place below the threshold of armed conflict, and therefore outside of the scope of the protections that IHL affords to civilians. Such conduct may also be difficult to classify from a legal perspective, contributing to the lack of clarity regarding the applicable legal framework and to the blurring of military and civilian roles in cyberspace.[60] While much of this activity is said to be conducted by proxies and other non-State actors, albeit sometimes reportedly on behalf of States, experts highlighted US CYBERCOM's strategy of Persistent Engagement and Defending Forward[61] as an example of military cyber operations meant to be conducted below that threshold.

[59] Offensive Security, Kali Linux.

[60] See also the discussion of the so-called 'grey-zone operations' in Section 2.C above.

[61] See US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, 2018, p. 6.

KEY TAKEAWAYS

- States and other stakeholders should continue to develop their understanding of the risk of civilian harm posed by the development of technology and work towards mitigating those risks.
- States should be aware of the risks associated with the employment of AI-enabled systems in military cyber operations, as well as of the growing attack surface caused by the expansion of the IoT.
- States should ensure that in the deployment of autonomous cyber systems, commanders or operators always retain a level of human control sufficient to allow them to make context-specific judgements to apply IHL.
- States and other stakeholders should continue to study the impact of the development of quantum computing, including the risks to civilians potentially posed by the quantum-enabled growth of computational power and the associated dramatic increase in the speed and scale of cyber and other operations.
- States should address the growing role of non-State actors in cyberspace, the impact that this evolution has on the changing nature of warfare, and the associated risks for civilians.

ANNEX 1: BACKGROUND DOCUMENT

This background document was prepared by Ewan Lawson, Military Adviser on Cyber, with a contribution from Laurent Gisel, Senior Legal Adviser, ICRC Legal Division. It aims to provide relevant material to support the discussions for the expert meeting. It does not necessarily represent the institutional positions of the ICRC.

TABLE OF CONTENTS

INTRODUCTION 37

I. UNDERSTANDING CYBERSPACE 37
Information and communications technologies 37
Cyberspace 38
Cyberspace and the information environment 38

II. CYBERSPACE AND INTERNATIONAL LAW 39
Application of international law to State use of ICTs 39
The protection afforded by IHL against the effects of cyber operations during armed conflicts 40

III. MILITARY CYBER OPERATIONS 42
Military roles and functions in cyberspace 42
Defining offensive cyber 43
Military offensive cyber processes 44

IV. CASE STUDIES 47
Operation Glowing Symphony 48
Russia-Georgia (2008) 49
Ukrainian power grid (2015–16) 49
Stuxnet 50

V. CONSIDERATIONS OF THE RISK OF CIVILIAN HARM AND ITS AVOIDANCE 51
Understanding the risk of civilian harm 51
Military approaches to assessing the risk of civilian harm 52
Approaches to minimize the risk of civilian harm 53

CONCLUSION 54

INTRODUCTION

The purpose of this background document is to provide an overview of military cyber operations and the avoidance of civilian harm as understood by the ICRC and hence a baseline for the expert meeting to be held in Geneva on 21–22 January 2020.

At least three States have declared the use of offensive cyber capabilities as part of military operations in an armed conflict,[62] and more States have declared the development of military cyber organizations and capabilities, including offensive capabilities. It is therefore essential to consider the risks to civilians and other protected persons and objects raised by military cyber operations. Cyber operations during armed conflicts indeed present a number of risks of civilian harm, including the dual military and civilian use of much of the physical and digital infrastructure and some of the data. The meeting will focus on ways in which civilian harm can be avoided or at least reduced in the conduct of military cyber operations during armed conflicts.

It is important however to underscore that any use of force by States – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law, in particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

This background document will first discuss the terminology surrounding cyberspace, including military cyber operations, focusing on the significance of the terms 'information and communications technology', 'cyberspace' and 'information warfare' (**Part I**). It will then give a short overview of the application of international law to cyberspace (**Part II**). Next, it will outline the context of the military use of cyberspace, particularly for offensive operations, focusing on those that are designed to cause disruptive or destructive effects, whether to a network or to associated physical infrastructure with a potential humanitarian impact (**Part III**). This will then be supported by an examination of a few relevant case studies, recognizing that the use of military cyber operations in armed conflict has to date been limited (**Part IV**). It will conclude with an analysis of the potential issues that such operations pose for the avoidance of civilian harm and how that can be assessed and mitigated (**Part V**).

I. UNDERSTANDING CYBERSPACE

INFORMATION AND COMMUNICATIONS TECHNOLOGIES

One of the challenges in developing a shared understanding of the risk of civilian harm from military operations in cyberspace is the lack of a truly shared lexicon. This is not merely a difficulty of language, as it also points to different perceptions of the significance of the digital environment and of the nature of the threat. Discussion in the international arena such as at the United Nations has focused on 'information and communications technologies' (ICT), the term that was used in resolution 53/70 which first brought the topic to the agenda of the First Committee on Disarmament and International Security in 1998.[63] ICT is generally taken as referring to 'computers, computer networks and systems, and disparate information distribution or delivery technologies such as land and submarine cables, satellites, the telephone, and even television'.[64]

[62] Australia, the UK and the US have all declared the use of offensive cyber capabilities, notably against the Islamic State group in Iraq/Syria, although details have not been published.

[63] UN General Assembly, Resolution 53/70, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70, adopted on 4 December 1998.

[64] C. Kavanagh, *The United Nations, Cyberspace and International Security: Responding to Complexity in the 21st Century*, UNIDIR, 2017, p. 7.

The terminology of ICTs continues to be used by the UN in the parallel Open Ended Working Group (OEWG) and Group of Government Experts (GGE) processes,[65] as well as in other fora.[66]

CYBERSPACE

However, one of the limits of the terminology of ICTs is that it focuses on the technology rather than recognizing the interdependence of those technologies with humans at both the societal and individual level. Despite having its roots in science fiction, the term cyberspace has gained increasing currency in many circles along with the prefix 'cyber'. Thus, the notions of cyber crime, cyber warfare and cyber espionage all arise from this root, although there are many different definitions for each of these and other cyber activities.[67]

Cyberspace is often described as a construct of connected layers which brings together its physical, virtual and cognitive dimensions. At its simplest this is three layers. The physical network layer is the hardware and connectivity that the network runs on and broadly comprises devices connected by cables and/or via the electromagnetic spectrum. As such, it has physical elements that are vulnerable to deliberate attack and to accidental damage; in 2011, Armenia was largely disconnected from the internet after a key cable through Georgia was cut with a spade by a 75-year-old woman looking for copper to sell.[68] The logical network layer is about the firmware, software and data; vulnerabilities in these are the focus of what are often targeted by cyberspace capabilities. Lastly, cyberspace also has a cyber-persona layer that reflects user accounts and the relationships between them. The ability to obfuscate and falsify identities in this layer has contributed to the challenge of accurately attributing the source of cyber attacks. It is also where, through social engineering, malicious actors can gain access to the logical network layer through methods such as 'spear phishing'.[69]

CYBERSPACE AND THE INFORMATION ENVIRONMENT

While not all States have identified cyberspace as a domain of warfare, even those that have done so recognize that it is inherently linked to the information environment. In some cases, its conceptualization even mirrors that of the three-layer model for cyberspace, with physical, informational and cognitive elements making up the environment.[70] However, the key connection is the way in which ICTs have transformed the information environment, particularly with regard to the dramatic increase these technologies have enabled in the speed of transmission and reach of information, but also their relative anonymity and the potential for obfuscation and deception.

Some States have therefore focused on the potential for information warfare to be the most significant change in contemporary and future armed conflict. They consider that the greatest threat in and through cyberspace is disruption to social, political and State stability through forms of information warfare.[71] Most notably, the Shanghai Cooperation Organisation (SCO) identified international information security as a key element of international security in its 2009 Agreement.[72] This document defines information warfare as:

'… confrontation between states in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems,

[65] UN General Assembly, Resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27, adopted on 5 December 2018; UN General Assembly, Resolution 73/266, *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266, adopted on 22 December 2018.

[66] See, for example, Declaration of the 11th BRICS Summit, 14 November 2019.

[67] For example, see South African Government, *South African Defence Review 2014*, pp. 2–18; Igarape Institute and The Sec Dev Foundation, *A Fine Balance: Mapping Cyber (In)security in Latin America*, Strategic Paper 2, June 2012, p. 4.

[68] D. Van Puvelde and A.F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, Polity Press, Cambridge, 2019, p. 29.

[69] *Ibid.*, p. 39.

[70] US Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, 25 July 2018, p. 2.

[71] See for example the Russian Federation, *Russian National Security Strategy*, December 2015, para. 21; The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, July 2019.

[72] Shanghai Cooperation Organisation Agreement on Cooperation in Ensuring International Information Security, Yekaterinburg, 16 June 2009.

psychologically manipulating masses of the population to destabilise society and the State, and also forcing the state to take decisions in the interest of the opposing party.'[73]

It further describes the development of information weapons as the greatest threat to international information security given the potential to disrupt a State's legitimate ability to defend itself, as well as highlighting concerns about the use of ICTs as a vehicle to disrupt societies. The draft *Convention on International Information Security (Concept)* put forward by Russia in 2011 has a similar definition.[74] Some Member States of the SCO also use cyberspace terminology in some of their official publications.[75]

II. CYBERSPACE AND INTERNATIONAL LAW

APPLICATION OF INTERNATIONAL LAW TO STATE USE OF ICTs

The two UN GA Resolutions establishing the OEWG and the GGE call for further study on *how* international law applies to State use of ICTs, and discussions are ongoing.

In these processes, States and other participants focused on the conclusions in the 2013 and 2015 GGE reports that international law and, in particular, the Charter of the United Nations are applicable to State use of ICTs, a position that was reaffirmed by many States. Delegates have affirmed that the agreements achieved through the 2015 report should not be rolled back even if discussions on how international law applies remains complex.[76]

Some States have continued to express concern that existing international law needs to be adjusted in order to become applicable to the ICT environment.[77] There have also been renewed calls for a new international convention.[78]

Turning more specifically to international humanitarian law (IHL), an increasing number of States and international organizations have affirmed that IHL applies to cyber operations during armed conflicts,[79] a view also held by the ICRC.[80] This mirrors the fact that a number of States and international organizations have identified cyberspace as a domain of warfare along with land, air, sea and, increasingly, outer space.[81]

Some States have suggested that the applicability of the law of armed conflict needed to be handled carefully, raising concern that to do otherwise carries the risk of cyberspace becoming a new battlefield, which should not happen under any circumstances.[82] Other States stated that acknowledgement of the applicability of IHL to cyber operations in armed conflict maintains ethical norms of behaviour and does not contradict efforts to stop conflict arising in the first place.[83]

[73] *Ibid*., Annex 1.

[74] The Ministry of Foreign Affairs of the Russian Federation, Draft Convention on International Information Security, 2011, Article 2.

[75] The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era*, July 2019.

[76] *Chair's Summary: Informal consultative meeting of the Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security*, 5–6 December 2019.

[77] Open-ended working group on Developments in the field of information and telecommunications in the context of international security, Submission by the Islamic Republic of Iran, September 2019.

[78] N. Achten, "New U.N. Debate on Cybersecurity in the Context of International Security", *Lawfare*, 30 September 2019.

[79] See, for example, United Kingdom of Great Britain and Northern Ireland, *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015*, September 2019.

[80] ICRC, *International humanitarian law and cyber operations during armed conflicts*, ICRC position paper, November 2019, pp. 5–6.

[81] US Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations*, 8 June 2018, p. I-2; NATO, Warsaw Summit Communique, 9 July 2016, para. 70.

[82] China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.

[83] Australia, Australian Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, September 2019.

In other forums, some States expressed opposition to cyber warfare and a cyber armed race,[84] or noted that there is no consensus on the applicability of IHL to cyberspace.[85]

For the ICRC, it is important to underscore that affirming the application of IHL to cyber operations during armed conflicts does not legitimize cyber warfare or encourage the militarization of cyberspace.[86] In fact, IHL imposes some limits on the militarization of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL.[87] Moreover, as already noted, any use of force by States – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law, in particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

THE PROTECTION AFFORDED BY IHL AGAINST THE EFFECTS OF CYBER OPERATIONS DURING ARMED CONFLICTS

Even among those States that have affirmed the application of IHL to cyber operations during armed conflicts, few have published detailed positions on how it should be interpreted or applied in practice. The rules on the conduct of hostilities are particularly relevant with regard to military cyber operations during armed conflicts. These rules aim to protect the civilian population against the effects of hostilities. They are based on the cardinal principle of distinction, which requires that belligerents distinguish at all times between the civilian population and combatants and between civilian objects and military objectives and that they direct their operations only against military objectives.[88]

As recalled in the most recent ICRC position paper on the issue,[89] affirming that IHL – including the principles of distinction, proportionality and precautions – applies to cyber operations during armed conflicts means that under existing law, among many other rules:

- cyber capabilities that qualify as weapons and are by nature indiscriminate are prohibited.[90]
- direct attacks against civilians and civilian objects are prohibited, including when using cyber means or methods of warfare.[91]
- acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited, including when carried out through cyber means or methods of warfare.[92]
- indiscriminate attacks, namely those of a nature to strike military objectives and civilians or civilian objects without distinction, are prohibited, including when using cyber means or methods of warfare.[93]
- disproportionate attacks are prohibited, including when using cyber means or methods of warfare. Disproportionate attacks are those which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[94]

[84] Statement by the Chinese Delegation at the 58th Annual Session of Asian-African Legal Consultative Organization (AALCO), 21–25 October 2019, Session on the Matter of International Law in Cyberspace.

[85] Statement by India at the 58th Annual Session of AALCO, 21–25 October 2019, Session on the Matter of International Law in Cyberspace.

[86] ICRC, *International humanitarian law and cyber operations during armed conflicts*, ICRC position paper, November 2019.

[87] See, among others, J-M. Henckaerts and L. Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. I: Rules*, ICRC, Cambridge University Press, Cambridge, 2005 (hereinafter ICRC Customary IHL Study), Rules 70 and 71; see also Art. 36 AP I.

[88] Art. 48 AP I; ICRC Customary IHL Study, Rules 1 and 7; International Court of Justice, *Legality of the threat or the use of nuclear weapons*, Advisory Opinion, 8 July 1996, para. 78.

[89] ICRC, *International humanitarian law and cyber operations during armed conflicts*, ICRC position paper, November 2019, pp. 5–6.

[90] ICRC Customary IHL Study, Rule 71.

[91] Arts 48, 51 and 52 AP I; ICRC Customary IHL Study, Rules 1 and 7.

[92] Art. 51(2) AP I; ICRC Customary IHL Study, Rule 2.

[93] Art. 51(4) AP I; ICRC Customary IHL Study, Rules 11 and 12. Indiscriminate attacks are those: (a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) which employ a method or means of combat the effects of which cannot be limited as required by international humanitarian law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

[94] Arts 51(5)(b) and 57 AP I; ICRC Customary IHL Study, Rule 14.

- during military operations, including when using cyber means or methods of warfare, constant care must be taken to spare the civilian population and civilian objects; all feasible precautions must be taken to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare.[95]
- attacking, destroying, removing or rendering useless objects indispensable to the survival of the population is prohibited, including through cyber means and methods of warfare.[96]
- medical services must be protected and respected, including when carrying out cyber operations during armed conflicts.[97]

In addition, all feasible precautions must also be taken to protect civilians and civilian objects against the effects of attacks conducted through cyber means and methods of warfare, which is an obligation that States must already implement in peacetime.[98]

As can be seen, most rules stemming from the principles of distinction, proportionality and precautions – which provide general protection for civilians and civilian objects – apply only to military operations that qualify as 'attacks' as defined in IHL.[99] The question of how widely or narrowly the notion of 'attack' is interpreted with regard to cyber operations is therefore essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.[100] Article 49 of Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or in defence". Rule 92 of the Tallinn Manual states that "a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[101] While this suggestion provides some clarity, it remains open to debate as shown in the commentary to that rule. In the ICRC's view, this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply. It also includes operations designed to disable a computer, or a computer network, whether the object is disabled through kinetic or cyber means.

The status of data is another issue of debate in terms of damage to civilian objects caused by military offensive cyber operations. While some scholars consider that data does not constitute an object for the purposes of distinction between civilian and military targets, others note that it has a value and that it can be destroyed and therefore should be considered.[102] While some States do not consider data to be objects,[103] others do, at least with regard to some data.[104]

It may also be noted that whether offensive cyber capabilities represent weapons, means or methods of warfare under IHL is debated.[105]

[95] Art. 57 AP I; ICRC Customary IHL Study, Rules 15 - 21.

[96] Art. 54 AP I; Art. 14 of Additional Protocol II of 8 June 1977 (AP II); ICRC Customary IHL Study, Rule 54.

[97] See, for instance, Art. 19 of the First Geneva Convention (GCI); Art. 12 of the Second Geneva Convention (GCII); Art. 18 of the Fourth Geneva Convention (GCIV); Art. 12 AP I; Art. 11 AP II; ICRC Customary IHL Study, Rules 25, 28 and 29.

[98] Art. 58 AP I; ICRC Customary IHL Study, Rules 22 - 24.

[99] The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

[100] ICRC, International humanitarian law and cyber operations during armed conflicts, ICRC position paper, November 2019, pp. 7–8.

[101] M.N. Schmitt (ed.), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017, p. 415.

[102] K. Mačák, *This is Cyber: 1+3 Challenges for the Application of International Humanitarian Law in Cyberspace*, Exeter Centre for International Law, Working Paper Series 2019/2, 2019.

[103] Danish Ministry of Defence, *Military Manual on international law relevant to Danish armed forces in international operations*, September 2016, p. 292.

[104] France, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*, September 2019, p. 15; Norwegian Ministry of Defence, *Manual of the Law of Armed Conflict*, 2013, para. 9.58.

[105] J.T. Biller and M.N. Schmitt, "Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare", *International Law Studies*, Vol. 95, 2019, pp. 179–225.

Addressing these debates is, however, outside the scope of the meeting. The meeting will focus on the avoidance of any form of civilian harm, whether or not these operations qualify as attacks under IHL and/or are designed or expected to cause physical effects. The terms 'cyber attacks' and 'cyber operations' are therefore used throughout the report in a technical (mainstream or colloquial) sense and not as they may be understood under IHL, unless specifically stated.

III. MILITARY CYBER OPERATIONS

The sensitivity and relative novelty of military cyber operations mean that the publicly available doctrine and policy are limited. Even where such documentation is available, it often refers to classified (and therefore unavailable) chapters or annexes that focus on the practical conduct of military cyber operations. This section will therefore bring together key themes from some of these sources in order to provide an overview of current thinking, while noting the limitations.

MILITARY ROLES AND FUNCTIONS IN CYBERSPACE

It has been argued by some researchers that over 100 States have military cyber organizations, although these take a range of forms and have a range of responsibilities.[106] 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. This has even included concerns about the risk to nuclear firing chains, which in turn has significant political implications for effective deterrence.[107] Thus, a primary focus for military cyber organizations is defence of their important operational networks. 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. This 'defend the nation' function is for example the role of National Cyber Protection Teams in the US Department of Defense Cyber Mission Force. However, in other States, such as France with the National Cybersecurity Agency (ANSSI) or the UK with the National Cyber Security Centre, this function is undertaken by agencies other than the armed forces, including those involved in law enforcement or intelligence and security. This task, whether focused on the armed forces' own networks or something broader, is sometimes referred to as computer network defence (CND) or a combination of network operations and defensive cyber operations (DCO). It is important to note, however, that the US lexicon for example refers to defensive cyber operations-response actions (DCO-RA) as part of this defensive role, although this refers to conducting offensive cyber missions against malicious actors who attack through cyberspace.[108]

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. With most armed forces and even non-State armed groups increasingly taking advantage of digital connectivity to enhance their operational performance, vulnerabilities in software and hardware provide opportunities for militaries to access those networks to collect data. As well as data on military capabilities connected to the network, the use of those networks for producing and sharing plans and other essential military information makes them an attractive target for military intelligence gathering. This is generally known as computer network exploitation (CNE) and is also a key part of the preparation for offensive cyber operations. Thus, the presence of a malicious actor on a friendly network

[106] N. Shachtman and P.W. Singer, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive", Brookings Institution, 15 August 2011.

[107] B. Unal and P. Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences*, Research Paper, Chatham House, London, January 2018.

[108] US Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations*, 8 June 2018, p. II-4.

can be an indicator of intelligence gathering or the preparation for something more disruptive or destructive which can in turn lead to inadvertent escalation.

Thirdly, some military cyber organizations have been tasked with the projection of national power in and through cyberspace through offensive cyber operations during armed conflicts. These can be conducted against targets from the strategic to the tactical level, including adversary weapon 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. They are therefore likely to be integrated into a nation's targeting processes although this is complicated by some other factors that will be discussed later in this paper.

DEFINING OFFENSIVE CYBER

As noted previously, one of the challenges of discussing aspects of cyber security more generally and military cyber operations is the extent of terminological confusion. There is no universally accepted definition for what constitutes an offensive cyber operation, and terms like 'cyber attack' are used by military officers, government officials, the media and the general public to describe everything from the theft of intellectual property, through online criminal fraud and deception, to website defacement and other disinformation activities, to disruptive and destructive attacks on elements of critical national infrastructure.

The UK MOD's Cyber Primer defines offensive cyber operations as "activities that project power to achieve military objectives, in or through cyberspace".[109] Similarly, US doctrine describes them as "missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR [combatant commander] or national objectives".[110] These definitions are particularly broad in character and thus are not necessarily helpful in understanding what is practically involved in an offensive cyber operation.

One potential definition for offensive cyber operations suggested by the author of this paper to address this is:

> the deliberate manipulation, addition or deletion of data in adversary (including civilian) networks in order to achieve physical and/or cognitive outcomes in support of military objectives.[111]

Outcome is meant here to refer to the ultimate outcome, not the direct effect of the operation. For instance, a cyber attack against a power grid that aims to undermine the confidence in the government is a cognitive effect according to the suggested definition. The same operation aimed at disabling the gates of a military facility to stop equipment being deployed is a physical outcome. This definition allows for the full range of potential military cyber operations and sources of harm to civilians to be included. Thus, a cyber operation directed at confusing GPS tracking in order to decrease an adversary's confidence in a military navigation system while not in itself having a physical effect, might have an inadvertent consequence that leads to civilian harm.

From this broad understanding of what is involved in conducting offensive cyber operations, Klimburg (2017) identifies three forms of offensive cyber operations.[112]

- Firstly, there are battlefield cyber operations that in many ways are a simple extension of electronic warfare practices designed to support other military activities in achieving physical effects. An example of this is the apparent blinding of a Syrian air defence system in order to allow Israeli aircraft to strike a nuclear facility in 2007.[113]
- Secondly, there is the use of offensive cyber capabilities to achieve, directly or indirectly, stand-alone physical outcomes as contrasted with supporting other military activities. There has not been much evidence of this to date, at least not on a publicly declared basis beyond the well-known examples

[109] UK Ministry of Defence, *Cyber Primer*, 2nd Edition, July 2016, p. 54.

[110] US Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations*, 8 June 2018, p. II-5.

[111] Given that participants may have different understandings of how offensive cyber operations are defined, this may be discussed during the meeting.

[112] A. Klimburg, *The Darkening Web: The War for Cyberspace*, Penguin Press, New York, 2017.

[113] L. Page, 'Israeli sky-hack switched off Syrian radars countrywide', The Register, 22 November 2007.

of Stuxnet and the reported damage to a German steel mill in 2014, where cyber attacks directly caused physical effects.[114] An example of an indirect attack is the Shamoon virus which affected Saudi Aramco, a major oil company, in 2012. Shamoon targeted the company's administration systems rather than its actual operational network, wiping data in a way that impacted significantly on the business and had the physical outcome of affecting the shipping of oil products.[115] In more recent years, there has been an increasing focus on the vulnerabilities in industrial control systems to achieve more significant effects in infrastructure such as the petrochemical industry, with the Triton attack identified in 2017 being an example of the potential risks.[116]

- Lastly, Klimburg identifies covert cyber actions focusing on persuasion and influencing as well as espionage. In 2011, the UK's Secret Intelligence Service corrupted the data on an Al Qaeda-linked website to change it from a bomb-making guide to a recipe for cupcakes, and in 2008, unknown actors defaced Georgian government websites as part of Russia's operations in South Ossetia.[117]

MILITARY OFFENSIVE CYBER PROCESSES

Having considered for what sort of purposes a party to a conflict might decide to resort to a military cyber operation, it is important to understand the sort of processes that militaries might utilize to identify and develop cyber capability. One model for this is the idea of a cyber kill chain, developed initially by Lockheed Martin.[118] While this framework has its critics, it is generally accepted as being a valuable analytical tool for all types of cyber operations. It has been described as follows:[119]

1. Reconnaissance

In this phase, the attacker identifies a target and gathers data. The information may include the nature of the organization and the organization's structure, systems and potential vulnerabilities. This phase can include simple steps such as finding email addresses and the functions of certain employees or finding the types of software stacks that are used.

2. Weaponization

This phase is about crafting tools that will be used later to gain access. These tools may use exploits for specific technical vulnerabilities. The attacker chooses the most efficient way of bundling the tool for subsequent delivery. This might be a malicious PDF file, a website that hosts malware (such as so-called watering hole attacks that target the site-specific audience), or an image, for example.

3. Delivery

The attacker delivers the tool to the target. There are many ways to do this, but they fall into two main categories: those that are automatic and those that require an action by the victim upon delivery.

4. Exploitation

Exploitation is the phase when a vulnerability in an application or in an operating system is leveraged to execute the attacker's code. This phase need not be automatic; it may happen when someone is tricked into performing certain actions, or it may even take place through the use of legitimate software installed on the system. The latter was among the techniques used by the NotPetya wiper, which harnessed the (legitimate) Windows Management Instrumentation.

[114] See R.M. Lee, M.J. Assante and T. Conway, *German Steel Mill Cyber Attack*, ICS Defense Use Case (DUC), SANS ICS, 30 December 2014.

[115] F.A. Rashid, "Inside the Aftermath of the Saudi Aramco Breach", Dark Reading, 8 August 2015.

[116] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker and C. Glyer (2017), "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure", FireEye Blogs, 14 December 2017.

[117] D. Gardham, "M16 attacks al-Qaeda in 'Operation Cupcake'", The Telegraph, 2 June 2011.

[118] C. Whyte and B. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, Abingdon, 2019, pp. 92–94. It should be noted that Lockheed Martin has registered this seven-step framework under a trademark.

[119] L. Gisel and L. Olejnik, *The potential human cost of cyber operations*, Expert Meeting Report, ICRC, Geneva, May 2019, Annex III background document, p. 56.

5. Installation

After the initial tool has been delivered and the vulnerability exploited, this initial tool may enable the installation of subsequent tools that will enable persistent remote access (e.g. trojans, implants or backdoors) and maintain that persistent access. That said, the specific features will depend on the particular circumstances, such as the malware that has been installed. After this phase, the initial compromise is turned into a more persistent one.

6. Command and control (C2)

When communication with the attacker's infrastructure is established through the installation of a remote-access tool (Phase 5 above), the intruders can issue commands to the malware installed in the victim's infrastructure. A number of techniques can be used to facilitate C2. Most commonly, remote servers are used to communicate with the tool. Alternatively, C2 channels can be established using removable media – such as a pen drive, in which case commands may only be delivered when the pen drive gets connected.

7. Actions on objectives

Once the attackers have obtained full access to the system inside the targeted network, they may perform various actions on the controlled system. For example, in NotPetya, the actions on objectives included the crippling of the Windows boot system (master boot record corruption). In the attacks on the power grid operators in Ukraine, actions on objectives encompassed the various activities leading to propagation within the system and the execution of commands that eventually resulted in power cuts. The malware implants installed (phase 5) may perform, or be used to perform, additional actions. For example, they may enable attacks on other systems in order to build persistence, exfiltrate data for use against other targets or be used as a bot in distributed denial of service (DDoS) attacks, if this was the aim of the operation. This phase may thus either be the final step, or it may be a step towards attacking further targets, either inside or outside the network.

For the attacker to complete the desired final step, it is typically necessary to have covered all seven phases. However, the phases do not always need to be executed in exactly the order described in the kill chain model (for example, the exploitation and installation phases may be repeated after command and control have been established). This underscores the dynamic nature of operations, where objectives may change, and attackers may have to take steps to maintain access. This is also why an espionage campaign may potentially transition easily into a disruptive or destructive campaign. This is possible, both technically and operationally, because of the ease with which cyber tools may be used, reused and modified, and because of their configurable nature.

It must be emphasized that this is a linear, albeit iterative, explanation of what is likely to be a more complex process with potentially multiple efforts to gain access to a specific network happening simultaneously. It is interesting to consider alongside a military targeting process such as that outlined in NATO Doctrine.[120] The targeting cycle consists of six phases, and it is possible to envisage how the cyber kill chain would link to this.

1. Commander's intent, objectives and guidance

At this stage, the operational commander will consider what objectives and effects he needs to achieve and how to assess when these have been achieved through measurements of effectiveness. Military cyber operators will at this stage be developing an understanding of adversary networks and considering what potential cyber capabilities exist or are in development. This overlaps with the reconnaissance and weaponization stages of the cyber kill chain.

2. Target development

In this phase, potential targets that might contribute to the commander's objectives are identified, analysed and validated, including for their legality under IHL. The potential for collateral damage will be considered at this stage, based on the guidance from the commander delivered as part of phase 1. Military cyber operators will

[120] See NATO, *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*, Edition A Version 1, NATO Standardization Office, April 2016.

be contributing to this through the use of information collected as part of the reconnaissance and weaponization stages, although it must be emphasized that this is very much an iterative rather than a linear process. In some cases, military cyber operators will be highlighting where they have both access and the capability to deliver an effect on a network; in others, they will be seeking to develop those as targets are identified. There will be a continuing dialogue throughout this stage between those considering the potential targets and means of attack and operational lawyers.

3. Capabilities analysis

In this phase, the full range of potential capabilities, including cyber capabilities, that will achieve the desired effects will be considered. A key element of this will be consideration of the potential for collateral damage of all the available options, and the assessment of which option could avoid or at least minimize such collateral damage. Military cyber operators will contribute to this process and in particular will be expected to identify how they can assure the commander of both the effectiveness of the capability and the extent of the risk of any unintended consequences. This information should have been developed as part of the weaponization phase of the kill-chain process outlined above.

4. Decision, planning and assignment

The commander will now decide what capabilities to assign to achieve specific objectives and assign these to various force elements, including military cyber elements. The military cyber force will engage with other elements of the force to ensure coordination.

5. Planning and execution

At this point the military cyber operators will be conducting the delivery, exploitation, installation, command and control, and actions on objectives phases of the cyber kill chain. In practice, it is likely that some of the first four of these activities will have taken place previously. The delivery of cyber capabilities requires preparatory activity that may need to be conducted prior to the execution phase of the targeting cycle.

6. Assessment

In the assessment phase, military cyber operators will review the employment of the cyber capabilities to understand and confirm what has been achieved and the extent of any unintended effects. This should feed back into future employment of cyber capabilities as well as cyber weapon development processes.

It can be seen that there is likely to be significant preparation required before a target can be considered for a cyber attack. As was noted previously, this preparatory activity overlaps significantly with CNE activity designed for broader intelligence purposes. In particular, a system access that has been developed for intelligence exploitation in the first instance may be considered as a vector for the delivery of effects. In such situations, military cyber operators will have to consider the intelligence loss/gain equation, given that such use would likely reveal the access to the adversary, allowing them to take measures to close it down. This lack of clarity regarding the reasons for the presence on the networks and systems of potential adversaries can also lead to concerns as to the final intention of that presence, which in turn can contribute to the risk of an escalatory reaction from the potential target.

The potential complexity of the intelligence requirement also means that preparation may well take place prior to the outbreak of hostilities in what is sometimes referred by some military planners as ‘Phase 0’. The nature of this activity also means that it may be led by a State’s intelligence agencies, which may or may not be military in nature. The significance of this is that much of the cyber kill chain activity may be undertaken outside of armed conflict, although the development during peacetime of cyber tools to be used during conflict must already consider all relevant IHL requirements for such subsequent use to be lawful.[121] It is also worth noting that this activity being conducted by intelligence agencies contributes to the sensitivity of military cyber operations and the lack of a detailed public conversation in most States. It also has implications for how States approach authorities for the conduct of military cyber operations.

[121] See, for example, Art. 36 AP I.

IV. CASE STUDIES

The number of occasions when States have publicly declared the use of offensive cyber capabilities in armed conflict has so far been limited to those by the UK, US and Australia, notably with regard to operations against the Islamic State group (ISg). The US-based Council for Foreign Relations maintains a database of all instances of publicly known State-sponsored cyber activity since 2005.[122] It suggests that some 25 States have sponsored or conducted cyber operations over this period although not all are military in nature or have taken place during armed conflicts, and many are linked to domestic political activity or to espionage or subversion activities.

This section will briefly consider four case studies in order to provide some context for the conduct of military cyber operations. It will first consider the only acknowledged use of cyber operations by States during an armed conflict, namely Operation Glowing Symphony against the ISg. It will then look at two cases of cyber operations taking place during ongoing armed conflicts, but whose attribution remains disputed: the cyber attacks that accompanied the international armed conflict between Russia and Georgia in 2008, which might also illustrate the potential for different perceptions of conflict in cyberspace, as well as the engagement of civilians outside the area of conflict; and the disruption of the Ukrainian power grid in 2015 and 2016 given its direct impact on civilians. It will finally consider Stuxnet as an example of a capability that appears to have been engineered to deliver a destructive effect but also to minimize the risk of collateral or cascading damage, though this operation was not carried out during an ongoing armed conflict.

It should be noted that there are other reported examples of the use of cyber operations during armed conflicts, and computer network exploitation techniques have been integrated with other military operations. For instance, an application developed by a Ukrainian military officer to improve the performance of artillery units was subject to an attack by a trojan which allowed those units to be geolocated and struck.[123] Further to this, Ukrainian units have seen soldiers' mobile phones hacked such that individuals and their families have been contacted with warnings prior to being subject to artillery strikes.[124]

As will be highlighted below, non-State actors have also made use of cyberspace as a vehicle for propaganda and recruitment in relation to armed conflicts. For example, in 2019 Hamas hacked the Israeli national broadcaster Kan. During a webcast of the Eurovision Song Contest, the images were interrupted and replaced with a faked warning from the Israeli Defence Forces (IDF) of incoming missile attacks. It then displayed faked images of explosions around the venue of the Song Contest and a warning that "Israel is not safe".[125] The IDF had previously conducted an airstrike on what it identified as a Hamas Cyber HQ in response to reported efforts of the latter to conduct a destructive cyber attack. Although the purported target of the Hamas cyber operation has not been publicly released, it is important to note that the targeting of the Hamas Cyber HQ building by kinetic means was based on intelligence gained as part of the IDF cyber defence effort.[126]

As part of the research for this paper, consideration was given to whether there was any evidence that a military cyber operation had been considered but then not deployed. Unsurprisingly, given the sensitive nature of such a decision, there is only a limited number of cases that have been discussed in the public domain. During the air campaign against Serbia in 1999, it has been suggested that the US considered cyber attacks but chose not to do so apparently due to concerns that the potential capabilities were untested. While generic legal advice was produced by the DOD at the time, no attack plan was apparently ever put forward for legal approval.[127] In 2003, while the Pentagon had the ability to conduct a significant offensive cyber operation against the

[122] See Council on Foreign Relations, Cyber Operation Tracker.

[123] A. Meyers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery", CrowdStrike Blog, 22 December 2016.

[124] A. Brantley and L. Collins, "A Bear of a Problem: Russian Tactical Cyber Operations", Modern War Institute at West Point, 29 November 2018.

[125] "Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions", BBC News, 15 May 2019.

[126] Z. Doffman, "Israel Responds to Cyber attack with an Air Strike on Cyber attackers in World First", Forbes, 6 May 2019.

[127] B. Graham, "Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia", The Washington Post, 8 November 1999.

Iraqi financial system, it chose not to do so as the result of concerns about the possible collateral damage.[128] It has been suggested that one reason was that Iraq's financial system was connected to a hub in France and the potential consequences could not be foreseen with a sufficient degree of certainty.[129] More recently it was reported that, in 2011, the US considered using cyber capabilities to disable the Libyan integrated air defence system. The option was not taken, and it has been suggested that this was due to the relatively short period to develop a bespoke capability and the risk of revealing US skills on a target that could be attacked in other ways.[130] This provides an interesting contrast with the more recent US targeting of military networks in Iran through cyber means rather than through a kinetic attack. It has indeed been suggested that it was a preferable way to respond after an Iranian strike against a US drone rather than to resort to a more conventional air strike. The media reported that while the impact on the system, which was alleged to have been used for monitoring and targeting commercial shipping in the Gulf, was expected to be temporary, it lasted longer than expected.[131]

OPERATION GLOWING SYMPHONY[132]

Established sometime in 2015–16, Operation Glowing Symphony was conducted by US CYBERCOM through a Joint Task Force (JTF) called Ares with the intention of curtailing the ISg's ability to exploit the internet for recruitment, propaganda and communication purposes. JTF Ares was placed under US CYBERCOM as it had a global remit unlike the other US headquarters engaged in the campaign against the ISg, which were regional in nature. Much of the documentation in the public domain is heavily redacted but it is possible from that which is available to draw some general insights.

Firstly, it was recognized that there were potential issues for policymakers where the ISg content or capability resided or depended upon infrastructure in other States including US allies. This reflects the challenge noted in some doctrine that cyberspace does not reflect geographic or geopolitical realities.[133]

Secondly, the available material indicates that the JTF was tasked and authorized to develop malware and other cyber capabilities to damage and destroy the ISg networks, computers and mobile phones.[134] It further notes the potential linkage to kinetic targeting, and it has been suggested that one cyber activity within the overall operation was designed to force the ISg leaders to use alternate headquarters locations which could then be struck and destroyed by conventional means.[135] Lastly, while it was led by US CYBERCOM, the documents indicate a clear role for allies and other members of the coalition. While both the UK and Australian governments have acknowledged their role in Glowing Symphony, publicly available documents also indicate a role for both Israel and the Netherlands, although the precise nature of this is unclear.[136]

The participants had declared the mission a success, noting that it had suppressed ISg propaganda, hindered communications and the ability to coordinate attacks and protected coalition forces on the battlefield.[137]

[128] J. Markoff and T. Shanker, "Halted '03 Iraq Plan Illustrates US Fear of Cyberwar Risk", The New York Times, 1 August 2009.

[129] L. Kello, *The Virtual Weapon and International Order*, Yale University Press, London, 2017, p. 125.

[130] E. Schmitt and T. Shanker, "US Debated Cyberwarfare in Attack Plan on Libya", The New York Times, 17 October 2011.

[131] See R. Millman, "US launches cyber-attack on Iranian weapons systems", SC Media, 24 June 2019; J.E. Barnes, "US Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say", The New York Times, 28 August 2019.

[132] See M. Martelle, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL", National Security Archive, 13 August 2018.

[133] US CYBERCOM, *Operations Order (OPORD) 15-0055: Operations Order in Support of Operation Inherent Resolve*, National Security Archive, 29 March 2015 [Redacted].

[134] US CYBERCOM to CDRUSACYBER, Subj: *CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space*, Secret//Rel to USA, National Security Archive, 5 May 2016 [Redacted].

[135] US CYBERCOM JTF-ARES, "United States Cyber Command Concept of Operations – OPERATION GLOWING SYMPHONY", Top Secret, National Security Archive, 13 September 2016 [Redacted].

[136] US Department of Defense, "Agreed Operation Glowing Symphony Notification Plan", Top Secret, National Security Archive, 4 November 2016 [Redacted].

[137] GCHQ, Director's Speech at Cyber UK 2018.

Researchers have noted a significant drop off in ISg online activity after November 2016 when the operation was formally launched.[138]

RUSSIA-GEORGIA (2008)

The conflict between Russia and Georgia in 2008 over the territory of South Ossetia has been described as the first in which offensive cyber activities were integrated with conventional military operations, although Russia denied any involvement and the cyber activities were publicly attributed to 'patriotic hackers'.[139] The main fighting took place between 7 and 16 August 2008 in all of the traditional domains of warfare with airstrikes, a naval blockade and hostilities between land forces on the ground. Russia's military strength in all three domains undoubtedly contributed to its ultimate success on the battlefield, but a campaign in cyberspace also contributed to Georgia's defeat. While it is difficult to assess the extent to which the cyber campaign was successful, its operational approach was delivered through a series of website defacements and distributed denial of service (DDOS) attacks that at one stage led to decreased functionality on some 35% of the Georgian internet, significantly contributing to impeding the military's and the government's ability to react, respond and communicate.[140]

There are two main considerations from this campaign. Firstly, it illustrates the use of cyber operations as a means by which to dominate the information landscape rather than a narrow mechanism to achieve discrete physical effects. Attacks on Georgian websites began some three weeks before the outbreak of conventional fighting, suggesting some effort to prepare the information battlespace. As well as inhibiting the ability of the Georgian government to act, these activities also contributed to a narrative that the Georgian government was not competent to protect its people. It has also been argued, however, that those carrying out these attacks chose not to attack facilities where the impact would have been chaos or injury, perhaps because they lacked confidence in the effectiveness of their offensive cyber capabilities, but more likely to keep the situation in those early weeks below the threshold which might have triggered further intervention. This appears also to have been reflected in the conventional campaign where strikes on a major oil pipeline were avoided.[141]

The second consideration is the role played by non-military personnel in the form of the supposed 'patriotic hackers'.[142] The Russian Federation has always denied any involvement with this informal movement which undertook much of the DDOS and website defacement activity. The conduct of offensive cyber activity in situations of armed conflict by individuals that are not State organs may need to be considered in any military response.

UKRAINIAN POWER GRID (2015–16)

It is not clear whether or not the attacks on the Ukrainian power grid in 2015 and 2016 took place within the realm of armed conflict despite the ongoing fighting in the east of the country. It is particularly significant, however, as it represents a direct attack on what appears to be civilian infrastructure. While the two attacks took place almost precisely a year apart, they were different both in their technical nature and their effect.

The first attack, in December 2015, was a sophisticated attempt to interfere with industrial control systems in electrical distribution centres and it led to between 230,000 and 1.4m people (depending on the sources) losing power for a few hours.[143] This attack has been linked to a group known as *Sandworm*, which at that time seemed to be using a trojan known as *BlackEnergy* to target businesses and governments in Ukraine, Poland and elsewhere. The attack was relatively sophisticated, with multiple actions that not only enabled the hackers to take control of circuit breakers but also struck the control stations' battery back-ups to impact

[138] See A. Alexander, *Digital Decay? Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, Program on Extremism, George Washington University, October 2017.

[139] D.M. Hollis, "Cyberwar Case Study: Georgia 2008", Small Wars Journal, 6 January 2011.

[140] S.P. White, *Understanding Cyber Warfare: Lessons from the Russia-Georgia War*, Modern War Institute at West Point, March 2018.

[141] D.M. Hollis, "Cyberwar Case Study: Georgia 2008", Small Wars Journal, 6 January 2011.

[142] S.P. White, *Understanding Cyber Warfare: Lessons from the Russia-Georgia War*, Modern War Institute at West Point, March 2018.

[143] C. Whyte and B. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, Abingdon, 2019, p. 110.

on the process of recovery. Having struck fifty distribution stations in 2015, the attack in December 2016 was targeted against one transmission station, albeit one that controlled more electricity than those 50 stations combined. Here the group used a programme known as CrashOverride, which appears to have been able to sabotage physical infrastructure without direct human involvement at the time of the effect on objective as had been required in the 2015 operation.[144]

Attribution of these attacks remains contested, but it has been suggested that they may have been part of a broader campaign to destabilize Ukraine and to make its government appear weak and vulnerable.[145] Alternatively, it has been suggested that the first attack may have been more commercially motivated as a threat to the Ukrainian authorities as they considered nationalization of power companies.[146] The effects on the electricity supply on these occasions was transient, with apparently no significant ill effects for the population. However, a longer-term power outage in a modern city would be at the very least disruptive with the potential for significant civilian harm. While this might not be the intent of such an attack, without careful consideration and technical understanding of the collateral risks, both direct and indirect/cascading, the unintended consequences could well be significant.

STUXNET

Like the attacks in Ukraine, the effort to undermine Iran's nuclear programme through the malware known as Stuxnet has never been formally attributed. However, publicly available sources suggest its deployment was part of an operation by the US and others known as Olympic Games. This attack was conducted outside an ongoing armed conflict and indeed it has been suggested that, at least in part, its use was to minimize the possibility of a conventional military confrontation.[147] Aside from the fact that this was the first publicly known attack to have directly caused a physical effect through cyberspace, it is also notable for the way in which it was designed to apparently minimize the risk of collateral damage, which is the reason for which it is discussed in this paper.

The malware was designed to surreptitiously alter the speed of centrifuges used by Iran for enriching uranium and open and close valves that linked the six cascades of centrifuges. At the same time, it provided false positive feedback to the operators with the intention of making them think the inevitable problems were the result of faulty equipment, poor engineering or incompetence.[148] While the ultimate impact on Iran's nuclear programme remains unclear, it has been suggested that it might have contributed to bringing Iran to the negotiating table and persuading Israel to show restraint rather than adopting a conventional military option.[149]

Stuxnet was extremely sophisticated. It utilized four or five 'zero day' exploits, was inserted across an airgap to a system not connected to the internet and was apparently configured only to work on that system in that location.[150] Thus, while the malware spread outside of the air-gapped network to infect computers across the globe, there are no other reported instances of damage.[151] It can be argued that malware customization like this is key to reducing the risk of civilian harm, but the more generic a target system is, the more challenging that becomes.[152] There is also the risk of reverse engineering, and it is significant that Stuxnet had a time-activated kill switch that stopped it replicating after June 2012, which may have been designed to minimize that risk.[153]

[144] A. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", WIRED, 20 June 2017.

[145] V. Zimmerman, "It's the Holiday Season Again. Will Ukraine Be Ready for the Next Cyberattack?", Atlantic Council Blog, 21 December 2017.

[146] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", WIRED, 3 March 2016.

[147] D.E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*, Scribe, London, 2018, p. 27.

[148] A. Segal, *The Hacked World Order*, Public Affairs, New York, 2016, p. 2.

[149] C. Sherman, "How We Got the Iran Deal and Why We'll Miss It", *Foreign Affairs*, September/October 2018.

[150] A. Segal, *The Hacked World Order*, Public Affairs, New York, 2016, p. 3.

[151] W. Jackson, "Stuxnet shut down by its own kill switch", GCN, 26 June 2012.

[152] L. Kello, *The Virtual Weapon and International Order*, Yale University Press, London, 2017, p. 124.

[153] W. Jackson, "Stuxnet shut down by its own kill switch", GCN, 26 June 2012.

V. CONSIDERATIONS OF THE RISK OF CIVILIAN HARM AND ITS AVOIDANCE

UNDERSTANDING THE RISK OF CIVILIAN HARM

Military offensive cyber operations during armed conflicts will be conducted under the operational procedures, rules of engagement and legal frameworks adopted by the State or non-State actor. However, as the case studies above illustrate, there remains a continuing risk of civilian harm. Attacks on electrical grids, such as that seen in Ukraine and the impact of WannaCry on the UK National Health Service in the UK, highlight the vulnerability of essential civilian services to cyber attacks.

The available policy and doctrine publications highlight that cyberspace is not contiguous with geographical or geopolitical boundaries and as such presents challenges for considerations of friendly, neutral and adversary territory. However, all note that cyberspace is essential for the functioning of global commerce as well as being key to critical national infrastructure, governance and defence activities. There is thus a general recognition of the civilian nature of much of cyberspace, including those parts that might be used by military and become dual-use, and the challenges this represents for discrimination in military cyber operations. Dual-use networks including those part of critical civilian infrastructure, even if exploited en route to a target that may lawfully be attacked under IHL during a conflict, remain vulnerable to inadvertent and/or unintended disruption. Furthermore, the dynamic nature of cyberspace, with software being upgraded frequently and new devices and new data being added, means that it can be difficult for those planning an offensive cyber operation to be completely confident of the environment in which they are operating.

In particular, there are risks of incidental effects, including indirect ones, arising from the nature of cyberspace and interconnectivity. Incidental (or collateral) effects are those effects on persons and objects that were not the targets of the cyber operation. As noted in Part II, the question of whether data are objects under the IHL rules governing the conduct of hostilities is subject to debate. Without prejudice to whether it corresponds to the notion of incidental harm under IHL, or whether it is under- or over-inclusive, the following suggestion may be a starting point for the discussion of direct incidental effects that might be caused by military cyber operations:

> Unintended harm to a computer or information system that is not the target of a lawful cyber operation. Where harm is defined as either the deletion, manipulation or alteration of computer code governing the operation of hardware or software that is not specifically intended … or the compromise of the integrity or availability of a computer network or data … that is not specifically intended … [154]

Incidental civilian harm might also be indirect (or reverberating or cascading), such as when an effect makes its way into subordinate, peer or higher connected networks, whether or not foreseen and expected, or when the harm to the computer, information system or data has cascading consequences in the physical world as illustrated in the case studies above.

All these effects might be expected (and therefore considered and minimized), but the risk of unintended and/or unexpected consequences may be exacerbated for example where the system targeted or incidentally affected has been unexpectedly modified between the design of the cyber capability and its employment.

As well as the risks inherent when systems and networks are targeted, it is possible for offensive cyber capabilities to be reverse-engineered or repurposed so that they can be reused. This is also the case for some traditional weapon systems, but the technical characteristics of cyberspace raise these concerns in a unique manner.[155] As noted earlier, while Stuxnet was designed to only operate on one specific target system, it

[154] S. Romanosky and Z. Goldman, "Understanding Cyber Collateral Damage", *Journal of National Security Law and Policy*, Vol. 9, 2017, pp. 244–245.

[155] L. Gisel and L. Olejnik, *The potential human cost of cyber operations*, Expert Meeting Report, ICRC, Geneva, May 2019, p. 7.

proliferated well outside that system, and one of the vulnerabilities it exploited, and which had been patched afterwards, was nevertheless used subsequently by other threat actors.[156]

MILITARY APPROACHES TO ASSESSING THE RISK OF CIVILIAN HARM

Avoiding or at least minimizing the risk of civilian harm entails both the verification that targets are indeed military objectives and considerations of collateral damage resulting from military action. This section focuses on the latter.

It has been argued that the interconnected nature of cyberspace along with the speed of activity and the way it does not necessarily reflect physical geography means that it is almost impossible to quantify and assess second and third order effects and hence assess the risk of collateral damage. However, States have asserted that indirect or cascading effects of cyber operations must be considered.[157] They have more generally held that all feasible precautions must be taken when carrying out cyber attacks to avoid or minimize civilian collateral harm, and that such harm must not be excessive.[158]

It has also been argued that while there might not be direct analogies with concepts such as 'blast radius' and 'probability of hit', it is possible to develop approaches to assessing the risks of collateral damage, and it has been asserted that a collateral damage estimate (CDE) must be made and risks and undesired effects must be mitigated.[159] One such approach is to consider the potential causes of incidental civilian harm from offensive cyber capabilities under four categories:

- **Errors** – Programming errors can be a significant source of unintentional disruptive behaviour. This underscores the importance of sound development, testing and validation procedures when States or other parties to armed conflict choose to develop or acquire military offensive cyber capabilities. It is of note that some States are developing 'cyber ranges' as part of this process. However, some producers of malware, including malware that might end up being used during armed conflict, might remain unconcerned about the risk of unintended harmful consequences; this may be compounded when expecting not to be identified or held responsible.
- **Target-specific dependencies** – These risks are based on properties and dependencies that are inherent to the target system and other systems that might present similar features. Thus, an in-depth understanding is required of the functions and dependencies of that system, its interconnections with other systems, the extent to which systems other than the target may present similar features, and the ensuing risk that the cyber tools planned to be used in the operation might also affect them if it spreads. It is recognized that this may represent a significant intelligence collection challenge as well as requiring detailed technical understanding.
- **Weapon-specific dependencies** – These risks reflect the intrinsic properties, execution behaviour or employment methodology of the weapon system. With offensive cyber capabilities it may prove difficult to control the distribution or spread, as was witnessed for example with Stuxnet. Particular importance should be given to minimizing such risks throughout the design of the capability and its employment so as to ensure that the capability can only affect the targeted system.
- **Other considerations** – With offensive cyber capabilities, this includes aspects such as intelligence loss or gain. While a successful operation might have the required effect, it might also reveal an access that was also being used to monitor the activities of a group carrying out illegal activities, which are now

[156] Kaspersky Lab, *Attacks with Exploits: From Everyday Threats to Targeted Campaigns*, April 2017, p. 23.

[157] France, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*, September 2019, p. 16; United States, Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2014–15, p. 6.

[158] *Ibid.*; Australia, *International Cyber Engagement Strategy*, p. 90 (proportionality only); New Zealand Defence Force, *Manual of Armed Forces: Law of Armed Conflict*, DM 69 (2 ed), Volume 4, 2017, paras 8.10.18(g) and 8.10.19; US Department of Defense, *Law of War Manual*, June 2015 (updated December 2016), paras 16.5.1.1. and 16.5.3.

[159] Danish Defence, *Joint Doctrine for Military Cyberspace Operations*, 1st edition, A (English), Copenhagen, September 2019, p. 25.

concealed. It should also be noted that the potential for cyber operations to achieve effects at a reduced risk of civilian harm when compared to kinetic operations may be a factor to be considered.[160]

The assessment of the risk of incidental civilian harm may be seen as a function of the calculation of the risks under these four headings balanced by any mitigations put in place. What is less clear is how military cyber operators go about making such assessments and what mitigations can be, and are, put in place in practice.

It is possible to consider a set of questions of the sort used by some militaries in their targeting processes to consider how it might be possible to begin to evaluate, and avoid or at least minimize, the risk of civilian harm from military cyber operations during armed conflicts:

- Can the target be positively identified? This would require positively identifying the target in the cyber-persona, physical infrastructure and/or logical infrastructure layers of cyberspace and considering how it can be affected in order to achieve the desired objective.
- Are there any civilians or civilian objects within the effects range of the weapons or tools that might be considered for use against the target? This would necessitate understanding whether there are any civilian IT or OT systems located on the same subnet or dependent upon connectivity with the target, whether any civilian systems or functions rely on the targeted system, and whether the cyber tools risk spreading to other networks or systems. In each such case, it would require an understanding of the nature, likelihood and magnitude of the incidental effect that may be expected on these civilian systems, including indirect effects.
- Can the incidental civilian harm (collateral damage) be avoided or at least reduced by using a different weapon, means or method and still achieve the goal? This would require assessing whether it is feasible to reduce the incidental civilian harm by, among others, exploiting a different vulnerability, adjusting the circumstances of the attack or launching a different operation and still achieving the objective. (Mitigations would be a vital consideration here.)
- What is the revised estimate of the risk of incidental harm to civilians and civilian objects after mitigation measures? This would require an ability to explain the risks of incidental civilian harm and the mitigations put in place to a decision maker.
- Given those estimates, does the attack still comply with the rule of proportionality? This would require assessment of whether the risk of incidental harm to civilians and civilian objects resulting from the proposed offensive military cyber operation is not excessive in relation to the direct and concrete military advantage anticipated (therefore requiring an assessment of the latter as well, though this is outside the scope of the meeting).

This framework suggests possible cyberspace-specific considerations that would be required to be assessed as part of collateral damage estimation methodologies (CDEM), but, like for kinetic operations, such an estimation is dependent on considerable intelligence gathering and analysis in support of military cyber operations. There is a potential risk of these standards being reduced in the context of high tempo operations during an armed conflict.

APPROACHES TO MINIMIZE THE RISK OF CIVILIAN HARM

There are a number of ways in which the risk of civilian harm from military cyber operations could be mitigated.[161] A particular risk is associated with the proliferation of cyber tools whether by design or inadvertently. There is no evidence that the WannaCry ransomware was designed to target the Health Service in the UK, but rather it appears to have been indiscriminate. Ensuring that an offensive cyber capability is designed to only operate against the target system is key, but built-in kill switches that for example disable the capability after a specified time period could contribute to decreasing the risk of repurposing and/or spread. Encryption of the capability would also contribute to reducing the risk of reengineering.

[160] G. Bertoli and L. Marvel, "Cyberspace Operations Collateral Damage – Reality or Misconception?", *The Cyber Defense Review*, Vol. 2 (3), Fall 2017, pp. 53–62.

[161] See, for example, L. Gisel and L. Olejnik, *The potential human cost of cyber operations*, Expert Meeting Report, ICRC, Geneva, May 2019, Annex III background document, pp. 75–77.

In addition to these active measures, some passive approaches should also be considered. Physical objects that have special protection such as medical facilities are physically marked to help identify them and ensure that they are not attacked during armed conflict. While there are potential technical issues, consideration should be given to digitally marking the equivalent facilities in cyberspace thus ensuring that there is no doubt as to their role. Further, States need to ensure that they protect essential civilian infrastructure as far as possible against threats in and through cyberspace. In some States this may need consideration of regulation given that ownership of much of the infrastructure lies in the hands of the private sector. Other measures that could be considered include segregating military from civilian cyber infrastructure and networks and segregating computer systems on which essential civilian infrastructure depends from the internet.[162]

Lastly, it can be argued that the key to reducing risk is through reducing the extent of cyber vulnerabilities. An international regime to disclose vulnerabilities to the relevant hardware and software producers could have a significant impact on risk in and through cyberspace.

CONCLUSION

There are important differences in the perception, approaches and terminology with regard to the military use of cyberspace. While a number of States oppose the militarization of cyberspace, military cyber operations are firmly established as a role for the armed forces of a number of States, although the span of responsibilities in cyberspace varies between States. Many militaries have responsibility for the defence of their own networks and systems, and some have been tasked with a broader role in defending national networks. Some States have been developing capabilities to take offensive action in and through cyberspace as adversary militaries become increasingly networked. The boundaries of what constitutes offensive cyber operations remain debated, but there is the potential to achieve destructive and/or disruptive outcomes. The conduct of such operations in armed conflict may involve preparatory measures on adversary networks prior to the outbreak of a conflict, which may raise a number of legal issues that are outside the scope of this meeting. This, along with the close relationship with cyber espionage, may see a significant role for intelligence organizations in some States.

At this time the only publicly declared use of cyber operations during armed conflicts has been those by the US, UK and Australia, most notably against the ISg. This was targeted primarily against propaganda facilities but was also apparently used to target individuals and facilities for kinetic strikes. The potential for destructive or other physical effects has been seen through other operations, most notably with the deployment of Stuxnet in Iran, the destruction of a German steel mill and the disruptive attacks against elements of the Ukrainian power grid.

In considering the employment of offensive cyber operations, it is important to recognize that the nature of networks and systems makes the challenge of identifying the risk of civilian harm and unintended consequences challenging. Military targeting and collateral damage estimation processes will need to be adapted to meet this challenge and technical methods and capabilities to support understanding and decision-making developed. Consideration will also need to be given to the tools and techniques that can mitigate that risk.

[162] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, ICRC, Geneva, 2015, p. 43.

ANNEX 2: SCENARIOS

Background

Alpha and Omega are adjacent States sharing a common land border and adjacent sea areas. Alpha has large conventional armed forces in all three traditional domains although much of its military capability is from the previous generation. Alpha Defence Intelligence Service (ADIS) acts as both the foreign intelligence and signals intelligence agencies for the State. Government and business have been relatively slow to embrace the digital revolution, but there is a basic level of connectivity and a significant sub-culture of hacktivists and cyber criminals. The Alpha Armed Forces (AAF) established a Cyber Command in 2017 which was initially given three core tasks: defending the AAF's networks and systems, supporting the government and business in defending against external cyber threats, and conducting cyber espionage. However, recent open-source reporting has suggested that Alpha also has a nascent offensive cyber capability built around exploits and accesses it has developed as part of its espionage programme.

Omega is smaller geographically and demographically than Alpha and lacks access to natural resources. As such it has developed an economy based on international finance and being a regional technology hub. It has relatively small conventional armed forces built around highly capable platforms and is integrated into a regional mutual security alliance. It is active internationally and, despite its small size, has been a regular contributor to UN peacekeeping missions. Omega's armed forces (OAF) established a Cyber Command in 2015 and, in addition to defending its own and government networks, immediately declared its intention to develop a military offensive cyber capability. This capability is supported by the Omega National Signals Intelligence Agency (ONSIA) which it has been reported in open sources has been a very capable actor in conducting cyber espionage and has developed a range of accesses and exploits.

There has been a significant dispute over the Alpha and Omega land border, and a Joint Commission has been in place for 20 years which has successfully dealt with immediate border issues but has failed to achieve a final agreement. Both States have, however, agreed since the commission was established to demilitarize the area five miles either side of the disputed border.

In early 2019, Omega announced that it had discovered oil on its territory close to the border with Alpha and that it would be developing the facility immediately. Alpha's government responded immediately, announcing that the oil was actually from its oilfields and that Omega was drilling under its territory and immediately moved troops inside the five-mile zone. Omega responded in kind and a standoff ensued while regional neighbours attempted to broker a solution to the dispute.

At the end of 2019, Omega announced the first commercial production of oil from its facility and this was followed by artillery exchanges across the border. It remains disputed who initiated these exchanges. They continued until January 2020, when three Omega soldiers were killed. The OAF then conducted a raid into Alpha territory with a small mobile force aimed at disrupting Alpha artillery fire and captured six Alpha soldiers. This led to an immediate escalation, with Alpha forces attacking across the border and advancing some 20 miles into Omega. Both sides have suffered significant casualties in the fighting but as of now the situation has stabilized. At sea, there were initially limited clashes but, as part of its assault, Alpha conducted an amphibious landing at a small port on the Omega coast and is now using this to support its land forces. Fighting continues along the line of confrontation.

Guiding questions

The aim is to use the following scenarios to discuss the risk that may be caused to civilians by military cyber operations. For each scenario we will consider the following questions:

- What risks of harm do civilians face from the cyber operation being considered, whether caused directly or through the indirect (or cascading or reverberating) effects of the operation? What are the risks in the physical domain? What are the risks in the digital/network domain?
- How can military cyber operators develop an understanding of the nature of the risk of civilian harm in this scenario and assess its likelihood, severity and potential impact?
- What choices might be made or measures put in place to avoid or at least reduce the identified risks of civilian harm?

The use of these hypothetical scenarios does not indicate any endorsement of the lawfulness of attacking the targeted facilities or assets or the choice of using military offensive cyber methods.

Scenario 1

The port of Raylan in Alpha is a medium-sized civilian commercial port that is the primary source of imports into the southern region of Alpha around Raylan. Raylan port is also being used to ship military logistic support, including ammunition, spare parts and fuel, by sea to the Alpha armed forces inside Omega territory through the small captured port. Interrupting these military supplies to the AAF would significantly impact on Alpha's ability to maintain its forces in the occupied area. Outgoing military supplies are largely containerized, being offloaded in the small captured port in Omega and delivered to the AAF logistic support bases in those containers.

Omega Cyber Command (OCC) has been tasked with conducting an offensive operation against Raylan port facilities in order to disrupt Alpha's logistics. It has gained an initial access to the container management system at the port and is proposing to delete and/or manipulate data in that system to misdirect containers.

Scenario 2

The Omega government have discovered that the AAF has been having problems sourcing a key component for the fuel for their multi-launch rocket system. They have decided to go into experimental production, and sources have indicated that the new component can give a significant boost to the system's range. Production is taking place in a light industrial zone in the town of Givens near the capital Alphaville. The plant had previously been used for the manufacture of agrochemicals and has been kept with this identity as far as any visible indicators are concerned. It is reported that the success of the trials means that the AAF is going to rush the component into production so that it can be deployed in the field within the next few months. For cyber security purposes, the plant does not have any direct connectivity to the internet but is operated via a local area network (LAN).

The OAF intelligence services have a HUMINT source within the plant. The OCC has been tasked with disrupting the plant in order to ensure that the fuel component cannot be produced. From their intelligence analysis, they have identified a vulnerability in the industrial control systems which manage the flow of the chemical into containers at the end of the production process and are developing a cyber capability to exploit that vulnerability.

Scenario 3

An elite unit of the AAF is operating from a barracks in a residential area in Givens. The unit is mobile in wheeled vehicles and is used to rapidly reinforce areas where the AAF's regular units are being defeated. Its higher levels of training and *esprit de corps* means that it has been particularly successful in battle against the OAF. It is thus not only a capable fighting force but one that is critical to the morale of the wider AAF. The senior leadership of the OAF have identified the unit as an important target and have set the objective of disrupting its ability to deploy to the front line. They are concerned however about the risks to civilians of a kinetic strike against the barracks facility.

The OCC has identified that the barracks has a fuel supply for its vehicles that is linked to a local distribution and pumping centre. They have so far managed to establish access to the network controlling the distribution and pumping centre and are now examining options for disrupting the fuel supply to the barracks through an offensive cyber operation.

Scenario 4

Alpha's strategic command and control functions are being conducted from an underground bunker which is part of the Office of the President in the centre of Alphaville. The facility has an unsophisticated network, although with cyber-security controls in place, and all of the business of the Office of the President is conducted from one small collection of servers located in the bunker. ONSIA have gained access to these servers and have been monitoring traffic between the Alpha government and its military high command, as well as broader government communications unrelated to the conflict.

Omega's government have made a calculation about the value of the intelligence and have decided to disrupt these communications both to impact directly on the conduct of military operations and to send a message to Alpha's government about the potential of its military offensive cyber capabilities. The OCC is working with the ONSIA to establish accesses that will allow this to be done.

Scenario 5

Whytecliff is the main town in the area of Omega that is controlled by Alpha troops, with a population of a few hundred thousand inhabitants. Alpha has established a command centre in a residential area of Whytecliff, which oversees notably the forces that have advanced 20 miles within Omega. For all its command and control activities, the command centre uses a specifically dedicated network that relies on power supplied by the general power grid. The command centre has generators, but a HUMINT source informs that they have been damaged by recent shelling and will not be fully operational again for the next 24 hours. The command centre has a secondary communication system through radio, but it is expected to be much less efficient.

Omega is ready to start a counteroffensive to retake the area captured by Alpha forces. Its cyber forces have been tasked to disrupt Omega's control and command communications when the counteroffensive starts. OCC cyber operators have been endeavouring to gain access to the network itself but have been unable to confirm that they can achieve the desired effects through a cyber operation directly against the network. However, they also gained persistent access to the control station for the main power line supplying the entire town of Whytecliff.

ANNEX 3: LIST OF EXPERTS

Invited experts

- **Mr Benjamin Ang**, Head Cyber Homeland Defence, Centre of Excellence for National Security, Nanyang Technological University, Singapore
- **Ms Karine Bannelier-Christakis**, Associate Professor & Department Director of Cyber Security Institute, University Grenoble Alpes, France
- **Mr Lior Bar-Lev**, Cyber Resilience Expert, Independent, Israel
- **Mr Pete Cooper**, CEO, Pavisade, United Kingdom
- **Mr Bart Hogeveen**, Head of Cyber Capacity Building, Australian Strategic Policy Institute, International Cyber Policy Centre, Australia
- **Dr Pavel Karasev**, Senior Researcher, Institute of Information Security Issues at Moscow State University, Russia
- **Mr Tobias Liebetrau**, Postdoctoral researcher, Centre for Military Studies, Department of Political Science, University of Copenhagen, Denmark
- **Mr Pete Renals**, Cybersecurity Analyst, USA
- **Ms Ellie Shami**, Cybersecurity Consultant and Automation Lead, Konfidas, Israel
- **Mr Vince Stewart**, LtGen (Ret), CEO, Stewart Global Solutions, LLC, USA
- **Ms Noëlle van der Waag-Cowling**, Cyber Strategist, Security Institute for Governance and Leadership in Africa, Stellenbosch University, South Africa
- **Mr Marcus Willett**, Senior Adviser for Cyber, International Institute for Strategic Studies, United Kingdom

ICRC

- **Dr Cordula Droege**, Chief Legal Officer and Head of the Legal Division
- **Dr Lindsey Cameron**, Head of the Thematic Unit, Legal Division
- **Mr Ewan Lawson**, Military Adviser on Cyber, Thematic Unit, Legal Division
- **Mr Laurent Gisel**, Senior Legal Adviser, Thematic Unit, Legal Division
- **Mr Kevin Chang**, Legal Adviser (Cyber), Thematic Unit, Legal Division
- **Mr Fabien Leimgruber**, Information Security Awareness Adviser
- **Dr Kubo Mačák**, Legal Adviser (Cyber), Thematic Unit, Legal Division
- **Dr Tilman Rodenhäuser**, Legal Adviser, Thematic Unit, Legal Division
- **Ms Delphine van Solinge**, Digital Threats Adviser, Protection Division
- **Ms Giulia Carlini**, Associate, Legal Division
- **Mr Giorgio Macor**, Associate, Legal Division

MISSION
The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

ICRC

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

4539/002 05.2021