ICRC EXPERT MEETING
14–16 NOVEMBER 2018 – GENEVA

THE POTENTIAL HUMAN COST OF CYBER OPERATIONS

Report prepared and edited by Laurent Gisel, senior legal adviser, and Lukasz Olejnik, scientific adviser on cyber, ICRC

Table of Contents

Foreword

One of the main aims of international humanitarian law (IHL) is to protect the civilian population from the effects of military operations. Cyber warfare is the subject of growing concern, and there is no consensus around the question of how IHL will protect civilians against its effects.

But what *are* the effects of cyber warfare on civilians? Since most known operations have been conducted outside conflict settings, the potential human cost of cyber operations in armed conflict is a matter of risk analysis.

To move towards a realistic assessment of the potential human cost of cyber warfare, the International Committee of the Red Cross (ICRC) invited scientific and cyber security experts from all over the world to share their knowledge. In a three-day meeting, experts analysed some of the most sophisticated known cyber operations, regardless of whether they occurred during conflict or in peacetime, focusing on the risk that cyber operations may result in death, injury or physical damage, affect the delivery of essential services to the population, or affect core internet services.

The meeting included participants working for global IT companies, cyber threat intelligence companies, computer emergency response teams, a national cyber security agency, participants with expertise in cyber security (including that of hospitals, electricity grids and other services), participants with expertise in the development and use of military cyber operations, lawyers and academics.

The rich discussions provided a nuanced picture of the risks that cyber warfare can entail for the civilian population. One of the main fears of those working on cyber warfare and IHL is perhaps the idea that in cyber space, the principle of distinction will be difficult if not impossible to uphold. Yet, the expert meeting showed that the global digital infrastructure that can be targeted through cyber operations is in fact rather resilient to widespread effects. While a number of the cyber attacks analysed were indiscriminate, many others have been precisely targeted from a technical perspective. Nonetheless, while many systems are resilient, others are particularly vulnerable, and health-care systems are among those. Furthermore, the threats are evolving at a faster pace than anticipated, and the most sophisticated cyber capabilities may be largely unknown.

Another area of concern highlighted in the meeting is the risk of proliferation of cyber tools, because they may linger in digital systems and can potentially be accessed from anywhere in the world, modified and reused.

In the view of the ICRC, many of the operations described in the report would be contrary to IHL if carried out during armed conflict. However, there is insufficient consensus today as to the interpretation of IHL in cyber space to provide clear legal protection for the civilian population.

We are grateful to the experts for having shared their deep knowledge and expertise. With this report, we hope to help develop a realistic picture of the risks to civilians that can arise from cyber warfare and to highlight the need to address those risks on several levels: through cyber security measures, but also through clarity and agreement about IHL as the most important international legal framework for the protection of civilians in armed conflict.

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

Executive summary

Cyber operations during armed conflicts: assessing the challenges for international humanitarian law

The use of cyber operations during armed conflicts is a reality. While only a few States so far have publicly acknowledged that they use them, cyber operations are a known feature of present-day military operations and the use of them is likely to increase in the future.

This new reality has triggered a debate regarding the rules of international law that apply to such operations. In this debate, the ICRC has recalled that during armed conflict, cyber operations are subject to the rules of IHL.[1] It is nevertheless clear that cyberspace and these new military operations raise a number of questions as to precisely how certain rules of IHL – which were drafted primarily with the kinetic realm in mind – apply to cyber operations.

Assessing these questions requires an understanding of the expected use and military potential of cyber technology. What aims may belligerents want to achieve by using new tools at the strategic, operational or tactical levels during conflicts? How does this new technology compare to other, existing means of warfare?

Furthermore, to assess how IHL protects civilians in armed conflict, and whether further regulation is needed, lawyers and policy makers require an understanding of the actual or potential human cost of cyber technologies. Indeed, one of the main aims of IHL is to protect civilians from the effects of military operations.

Purpose and scope of the meeting

As part of its mandate to work for the clarification of IHL and, if necessary, prepare any development thereof, 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, technical, military and humanitarian considerations, which are interrelated.

To develop a realistic assessment of cyber capabilities and their potential humanitarian consequences in light of their technical characteristics, the ICRC brought together scientific and cyber security experts from all over the world to share their knowledge about the technical possibilities, expected use, and potential effects of cyber operations. The three-day meeting drew on the expertise of participants working for global IT companies, cyber threat intelligence companies, computer emergency response teams, a national cyber security agency, participants with expertise in cyber security (including that of hospitals, electrical grids and other services), participants with expertise in the development and use of military cyber operations, lawyers and academics.

States and militaries remain reluctant to disclose their cyber capabilities, including the details of cyber operations conducted in the context of armed conflicts, and little is known about the few acknowledged cases. Therefore, the experts discussed a number of the most sophisticated known cyber operations, regardless of whether they occurred in the context of an armed conflict or in peacetime. Examining the technical features of these attacks and the specific vulnerabilities of the respective targets provides a powerful evidence base for what is technically possible also during armed conflict.

The meeting focused in particular on the risk that cyber operations might cause death, injury or physical damage, affect the delivery of essential services to the population, or affect the reliability of internet services. It looked at the specific characteristics of cyber tools, how cyber threats have evolved, and the cyber security landscape.

Approaching the subject from a humanitarian law and humanitarian action perspective, the ICRC seeks a sober and – to the greatest extent possible – evidence-based understanding of the risks of cyber

[1] See in particular: ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts*, ICRC, Geneva, 2015, pp. 39–44 (hereinafter ICRC 2015 IHL Challenges report) (all web addresses accessed April 2019). The restrictions imposed by IHL do not legitimize the use of force in cyber space, which remains governed by the United Nations Charter.

attacks[2] for the civilian population. The meeting allowed the ICRC to confirm much of its own research (submitted in the background paper, included as Annex 3), and to supplement it with highly valuable additional expert knowledge. The meeting was extremely useful in that it contributed to a nuanced picture of cyber operations, demystifying some of the assumptions that often surround discussions on cyber warfare.

Areas of concern

Discussions helped to put the spotlight on four areas of particular concern in terms of the potential human cost of cyber operations:

a) the specific vulnerabilities of certain types of infrastructure
b) the risk of overreaction due to potential misunderstanding of the intended purpose of hostile cyber operations
c) the unique manner in which cyber tools may proliferate
d) the obstacles that the difficulty of attributing cyber attacks creates for ensuring compliance with international law.

a) Specific vulnerabilities of certain types of infrastructure: cyber attacks that may affect the delivery of health care, industrial control systems, or the reliability or availability of core internet services

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

Cyber attacks that may affect the delivery of health care

The health-care sector is moving towards increased digitization and interconnectivity. For example, hospital medical devices are normally connected to the hospital's information technology (IT) system to enable automatic electronic filing. Connected biomedical devices, such as pacemakers and insulin pumps, make it possible to remotely monitor individual patients' health as well as the functioning of the medical devices themselves.

This increased digital dependency, combined with an increased 'attack surface', has not been matched by a corresponding improvement in cybersecurity. Consequently, this infrastructure is particularly vulnerable, with potentially serious consequences for health and life.

Cyber attacks against industrial control systems, including those used in critical civilian infrastructure

Industrial control systems are protected by complex safety mechanisms and often have built-in redundancy to guarantee safety and reliability. For example, electrical networks are grids with multiple power sources to avoid widespread effects when one of their parts is affected. Nonetheless, attacks on specific nodes might still cause a significant impact, such as if a critical system (like a hospital) depends on a specific sub-system or node, or because they have cascading harmful consequences.

Carrying out a cyber attack against an industrial control system requires a certain expertise and sophistication, and, often, custom-made malware. Such attacks have been less frequent so far than other types of cyber operations. Nonetheless, their frequency is reportedly increasing, and the severity of the threat has evolved more rapidly than anticipated only a few years ago. There is a risk that tools developed by the best-resourced actors may be repurposed or purchased by other actors who lack the expertise required to develop them from scratch. Moreover, there is a possibility that a number of undetected actors are capable of attacking industrial control systems.

Cyber attacks that may affect the reliability or availability of internet services

Cyber attacks that disrupt core internet services, such as the domain name system (DNS), which supports communications on the internet, or disrupt the functioning of major cloud services, may impact all services that rely on them. However, the risk of seriously compromising these core internet services was assessed by the experts as unlikely at the present moment thanks to the high degree of redundancy in the DNS and because major cloud providers tend to offer high security standards. If,

[2] The terms "cyber attacks" and "cyber operations" are used throughout the report in a technical (mainstream or colloquial) sense and not as they may be understood under international humanitarian law (IHL), unless specifically stated (see the first paragraph of Session 1 below for more details).

however, such disruption were to occur, it could have widespread and potentially serious consequences, for example when life-saving services such as ambulances rely on the cloud.

Finally, "distributed denial of service" (DDoS) attacks have been used against services provided by governments for the population. Such attacks are carried out through increasingly large botnets. The arrival of the internet of things will further increase the number of connected devices that could be used in such attacks. Furthermore, DDoS attacks might have a wider impact than expected by their author, in particular when information about the targeted network is incomplete.

b) Risk of overreaction due to the potential misunderstanding of the intended purpose of hostile cyber operations

Cyber operations can be broadly divided into two categories, depending on their purpose:

- activity encompassing reconnaissance, surveillance and the exfiltration of data and information, for example for espionage, often referred to as computer network exploitation (CNE), or "access operations"
- activity to generate effects on a targeted system or device, such as tampering with data integrity (deletion, modification), affecting availability (disabling, including for prolonged periods of time), or causing physical effects, such as damaging the system, often referred to as a computer network attack (CNA), or "effects operations".

The distinction is primarily one of purpose. From a technical perspective, the initial steps of a CNE and a CNA to gain and maintain persistent access to the target may be identical. CNEs can then be turned into CNAs relatively simply, mostly through the use of specific payloads of a different nature. While the initial steps of the attacks may be tracked, it is often difficult to fully assess the attacker's purpose until the effect on the end target is actually achieved.

When the target does not know the actual purpose of the operation, its reaction may be to consider the potential worst-case impact that the attacker could achieve though a CNA and react in a stronger manner than it would have if it had known that the intended purpose of the attack was CNE. This escalation risk factor may give rise to a potentially harmful over-reaction.

c) Proliferation of cyber tools

A third concern is the proliferation of cyber tools – an issue that in some respects raises concerns similar to those that may exist with regard to weapons proliferation or the proliferation of dual-use technology, although the specific nature of cyber tools must be taken into account.

Cyber tools and methods can proliferate in a unique manner that is difficult to control. First, cyber space is a global domain: provided that the attacker can overcome the cyber security and defence measures in place, any network node and information residing on the network can be accessed from anywhere in the world. At the same time, cyber tools can be repurposed or reengineered. The combination of these two characteristics means that when cyber tools have been used, stolen, leaked or otherwise become available, actors other than those who developed them might be able to find them, reverse engineer them, and reuse them for their own purposes.

Finally, the fact that cyber tools and methods can be repurposed and reused is one of the factors making rapid and reliable technical attribution of cyber attacks a challenging process.

d) Attribution of attacks

While not a primary focus of the meeting, the discussions also touched upon the anonymity of attacks and the difficulty to attribute them to a specific actor, which is a fourth area of concern.

Cyber space is a complex domain where multiple actors operate: individual hackers; criminal groups, potentially motivated by financial gain; States; non-State armed groups; and other non-State actors. Actors may also cooperate: for example, States may buy cyber tools or have an operation performed on their behalf against a target they have identified.

Digital forensics and the capabilities of attribution of malicious cyber activity appear to be improving. Nonetheless, the ability of threat actors to obscure or effectively hide the origin of their operations on the internet, compounded by the ability to buy, repurpose or reengineer cyber tools developed or used by other actors continues to make it difficult to rapidly and reliably attribute cyber attacks to a specific actor. This hampers the possibility to identify actors who violate IHL in cyberspace and hold them responsible. This is a concern because to hold such actors responsible is one way to ensure compliance with IHL. It may also lower the threshold of using cyber attacks and of using them in violation of international law, because attackers can deny responsibility.

Cyber operations during armed conflicts: implications for international humanitarian law

It is well-established that international law applies to cyber operations. More specifically, IHL and its principles of distinction, proportionality, precaution, military necessity and humanity restrict the use of cyber means and methods during armed conflict. Further discussions may however be needed to clarify how IHL applies and whether it is adequate and sufficient or requires further development, building on existing law.

The meeting helped to clarify which areas of humanitarian concern should be the focus of attention. In brief, based on the detailed knowledge of cyber operations during peacetime, and somewhat lesser knowledge of cyber operations in times of armed conflict, the following picture emerges:

Distinction in cyber space

First, cyber attacks are not necessarily indiscriminate. As the report illustrates in more detail, cyber tools can be designed to self-propagate or not. Even if they self-propagate and cause cyber security concerns for all those infected, they can be designed to only cause damage to a specific target. While some self-propagating malware that caused indiscriminate harmful effects has made headlines, many cyber operations have in fact been rather discriminate from a technical perspective (which does not mean they were lawful).

Furthermore, certain types of cyber attacks require custom-made cyber tools, such as those that would aim to cause physical damage to industrial control systems. In many cases this would also effectively hamper the ability to carry them out in a large-scale indiscriminate manner.

This is important from an IHL perspective, because contrary to the assumption often heard that the principle of distinction might have become meaningless in cyber space because of the interconnectivity that characterizes it, not all offensive cyber tools are inherently indiscriminate. On the contrary, they may well be very precisely tailored and create effects on specific targets only.

Highlighting the potential human cost

Secondly, and of equal importance, it is nonetheless clear that cyber tools can cause substantial damage and can be – and have sometimes been – indiscriminate, and that certain systems are particularly at risk, first and foremost, perhaps, health-care systems. Moreover, the threats that can be observed have been evolving faster than anticipated, in particular regarding attacks against industrial systems. Finally, much is still unknown in terms of the rapid evolution of the technology, the capabilities and the tools developed by the most sophisticated actors, and the extent to which the increased use of cyber operations during armed conflicts might be different from the trends observed so far. In other words, while the risk of human cost based on current observations does not appear extremely high, especially considering the destruction and suffering that conflicts always cause, the evolution of cyber operations still merits close attention due to existing uncertainties and the rapid pace of change.

Legal protection through IHL

Many of the attacks described in the report targeted or indiscriminately affected civilian infrastructure. In the view of the ICRC, if carried out in times of armed conflict, such attacks would be prohibited. First of all, direct attacks against civilian infrastructure and indiscriminate attacks would be prohibited. Secondly, even if the infrastructure or some parts of it had become military objectives (such as a part of an electricity grid), IHL would require that only this part be attacked, and that there be no excessive damage to the remaining civilian parts. Thirdly, IHL would require parties to the conflict to take all feasible precautions to avoid or at least minimize incidental harm to civilians and civilian objects. Finally, even when they do not amount to attacks under IHL,[3] such operations might also be prohibited by the specific protection afforded by IHL to medical facilities or objects indispensable to the survival of the population. These are powerful protections that remain entirely relevant in view of the technical characteristics of cyber operations. For IHL to truly provide legal protection to civilians against the effects of cyber warfare, however, States must commit to its applicability and to an interpretation of its rules that is effective for the protection of civilians and civilian infrastructure. In particular, it would require a clear recognition that cyber operations that impair the functionality of civilian infrastructure are subject to the rules governing attacks under IHL.[4] This report will hopefully help illustrate the need for such an interpretation to ensure that civilian infrastructure is protected.

[3] Under IHL, "attack" has a specific meaning which would not encompass all cyber operations that are referred to as cyber attacks in a colloquial sense. See Chapter 2(c) below and Part 3(f) in the background document contained in Annex 3.

[4] See ICRC 2015 IHL Challenges report, p. 41 (see note 1 above).

Avenues that could be explored to reduce the potential human cost of cyber operations

Cyber security measures

Beyond the restraints imposed by IHL upon those carrying out cyber operation, it is critical to enhance the cyber security posture and resilience of the actors potentially affected. While cyber security and defence are constantly improving, older systems with outdated or even non-existing cyber security are particularly vulnerable to cyber attacks and will remain a concern in the years to come. Both the public and private sectors have a role to play through industry standards and legal regulation.

In the health-care sector, for instance, the regulatory environment should be adapted to the increased risk, such as through standardization requirements, with a view to ensuring resilience in the event of a cyber attack. Cyber security needs to be taken into account in the design and development of medical devices and updated throughout their lifetime, no matter how long they last. Similarly, for industrial control systems, industry standards, whether imposed or self-imposed, are critical. This includes reporting incidents and sharing information between trusted partners.

In terms of IHL, parties to armed conflicts must take all feasible precautions to protect civilians and civilian objects under their control against the effects of attack. This is one of the few IHL obligations that States must already implement in peacetime.

Disclosing vulnerabilities

The preferred option for enhancing the safety of cyber space should be disclosing vulnerabilities to the appropriate software developer so that the vulnerabilities can be fixed. Some States have therefore put in place equity processes to balance competing interests and risks and decide whether to disclose the vulnerabilities they identify.

Measures to prevent proliferation

Those who develop cyber weapons should consider creating obstacles in order to make repurposing difficult and expensive. While it is hardly possible from a technical standpoint to guarantee that malware cannot be repurposed, methods like encrypting its payload and including obstacles in different components of the code, for example, could raise the bar in terms of the expertise required to reengineer malicious tools. While there is currently no express obligation under IHL to create obstacles to the repurposing of cyber tools, this could prevent at least some actors from doing so and therefore reduce the risk of subsequent misuse that their proliferation entails. The unique way in which cyber tools proliferate also raises the question of whether existing law is adequate or sufficient to address this phenomenon.

Marking of certain civilian infrastructure

Another avenue, which builds on existing international law, could be to create a "digital watermark" to identify certain actors or infrastructure in cyber space that must be protected (such as objects that enjoy specific protection under IHL). The aim would be to help their identification and prevent them from being targeted during armed conflicts. The potentially positive effects in terms of protection against unintended harm by law-abiding actors would however need to be balanced against the risk of disclosing information on critical infrastructure to potential adversaries, including criminals. The prospects of positive effects might depend in part on attribution becoming easier.

Improving attribution and accountability

Finally, enhanced attribution capacities would help ensure that actors who violate international law in cyber space can be held accountable, which is a means to strengthen compliance with the law and more generally encourage responsible behaviour in cyber space.

Way forward

The use of cyber operations in armed conflict is likely to continue and might remain shrouded in secrecy. Analysing its consequences is a complex and long-term endeavour that requires multidisciplinary expertise and interaction with a wide variety of stakeholders.

Building upon the conclusions reached at the expert meeting, the ICRC would like to pursue the dialogue with governments, experts and the IT sector. It looks forward to the feedback to this report to continue to follow the evolution of cyber operations, in particular during armed conflicts, and their potential human cost, explore avenues that could reduce them, and work towards a consensus on the interpretation of existing IHL rules, and potentially the development of complementary rules that afford effective protection to civilians.