International Review of the Red Cross (2022), **104** (919), 1501–1505.
Selected Articles
doi:10.1017/S1816383121000540

IRRC

REPORTS AND DOCUMENTS

Executive Summary: Avoiding civilian harm from military cyber operations during armed conflicts

In January 2020, the International Committee of the Red Cross (ICRC) invited experts from various parts of the world to share their knowledge on practical issues for the implementation of international humanitarian law (IHL) in military cyber operations. 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 emerged 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.

Executive Summary[1]

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.

1 The report from which this Executive Summary is extracted was prepared by Ewan Lawson, military adviser on cyber, and Kubo Mačák, legal adviser, ICRC. The full report is "Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21–22 January 2020 – Geneva", available at: https://shop.icrc.org/avoiding-civilian-harm-from-military-cyber-operations-during-armed-conflicts-icrc-expert-meeting-21-22-january-2020-geneva-pdf-en. The ICRC Humanitarian Law & Policy blog ran a series of several posts on the same theme, "Avoiding Civilian Harm During Military Cyber Operations", available at: https://blogs.icrc.org/law-and-policy/category/special-themes/avoiding-civilian-harm-during-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, all feasible precautions must be taken to avoid or at least minimize incidental civilian harm. 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.