BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

CSDS POLICY BRIEF • 14/2022

The digitalisation of armed conflicts: Three humanitarian priorities

By Peter Maurer | 13 June 2022

Key Issues

- The use of new technologies in warfare poses new risks to people, such as cyber operations disrupting civilian infrastructure, disinformation undermining trust in societies, hate speech fuelling violence, and data breaches against humanitarian organisations putting vulnerable people at risk and undermining humanitarian action.
- States should interpret – and apply – existing rules in a manner that ensures adequate and sufficient protection for civilians and civilian infrastructure, information and communication technology (ICT) systems and data in our ever-increasingly digitalised societies.
- Academia, tech companies, states and humanitarians should work together to better understand the impact of misinformation, disinformation, and hate speech in contexts affected by armed conflict and violence, and to identify ways to address it.
- The humanitarian community must join forces – and find partners – to ensure the best possible protection against cyber operations targeting humanitarian operations and personal data entrusted to us.

As the world digitalises at unprecedented speed, digital technologies are also changing warfare and the needs of people affected by it, a trend that will only accelerate in the coming years. Technological advances have the potential to help us improve the lives of millions of people and alleviate suffering, for instance by analysing huge amounts of data to identify missing persons. In situations of armed conflict and violence, people ask the International Committee of the Red Cross (ICRC) for internet connectivity to contact families or access lifesaving information. But new technologies also pose new risks to people: cyber operations disrupting civilian infrastructure, disinformation undermining trust in societies, hate speech fuelling violence, and data breaches against humanitarian organisations putting vulnerable people at risk and undermining humanitarian action – all of this has made headlines in recent months. Here are three issues we need to prioritise to mitigate the most serious humanitarian consequences of the digitalisation of armed conflict and preserve a digital humanitarian space.

Protecting civilian populations against the harmful effects of cyber operations

Today, data and digital technologies have become a key element of strategic competition between states – and also of warfare. An increasing number of states are developing information and communication technology (ICT) capabilities for military purposes and their use in armed conflicts is becoming more likely. Over recent years, numerous cyber incidents have occurred and harmed civilian infrastructure. These incidents

often occur in contexts of political tension or ongoing armed conflict. While some see cyber operations as a means to help avoid traditional uses of force, others have warned that cyber operations conducted by States risk escalating political crises into wars – and war means destruction, devastation, and suffering of civilians.

As humanitarians, we have raised concerns – and states have recognized – that ICT activity against critical civilian infrastructure has become "increasingly serious" and their "human cost [...] could be substantial". There is a real risk of "potentially devastating [...] humanitarian consequences" when cyber operations are conducted against critical civilian infrastructure. Think about cyber operations halting hospital services in the middle of a global pandemic or armed conflict preventing people from getting medical treatment, or cyber operations causing physical damage to industrial plants or nuclear facilities. This is not science fiction – we have seen such operations over the past decade.

In addition to these "worse case" events, in recent years many cyber operations have been designed to disrupt or disable critical civilian infrastructures, governance services, or economic activity without necessarily causing consequences traditionally associated with "physical" or "kinetic" warfare. For instance, electricity networks have been disabled, digital governance services disrupted, and company data encrypted without necessarily causing physical damage or bodily harm to humans. We fear that cyber operations could be used to force political or military concessions, potentially escalating into states holding each other's civilian infrastructure or data "hostage", with serious impacts on civilians.

At times, it is alleged that cyberspace is a lawless space, a digital "wild west". The reality is far from it, especially if we think about cyber operations carried out by states or state-sponsored actors. States unequivocally agree that "international law, and in particular the Charter of the United Nations is applicable" in the ICT environment. Discussions in the diplomatic forums have developed in parallel to in-depth reflections in academic circles. For instance, legal experts involved who developed the Tallinn Manual 2.0 on international law applicable to cyber operations have provided significant guidance on how existing rules of international law should be interpreted to prevent the most severe consequences for the civilian population. For over two decades, the ICRC participated in such discussions and consistently held that there should be no doubt: in times of armed conflict, international humanitarian law – also known as the law of armed conflict – imposes clear limits on cyber operations.

States have come a long way towards affirming the application of existing rules of international (humanitarian) law in cyberspace. This is commendable – but it can only be a first step. To ensure that people affected by armed conflict are protected against harmful cyber operations, concrete legal and policy steps are needed to bridge gaps between theory and practice, between battle-proven rules and new realities;

- In times of armed conflict, international humanitarian law contains long-standing protections for people from all forms of violence. States should interpret – and apply – existing rules in a manner that ensures adequate and sufficient protection for civilians and civilian infrastructure, ICT systems and data in our ever-increasingly digitalised societies.
- The law of armed conflict has to be operationalised in the ICT environment. Cyber operators need clear rules and procedures, and they need to adapt their tools and targeting processes to cyberspace. Malware does not necessarily spread and affect civilian infrastructure indiscriminately – programmers have the means to prevent this.
- Societies need to take measures to protect civilian infrastructure and populations from cyber threats. Cyber resilience and redundancy in essential networks and services are essential, and so is the segregation of certain networks (e.g. military ones from civilian ones) or separate cloud services for essential services (e.g. medical ones).

Mitigating the spread of harmful information, especially in times of armed conflict

Over the past decade, we have also seen how digital communication systems have contributed to the spreading of harmful information online – in particular misinformation, disinformation, and hate speech. Unfortunately, there has been limited attention given to how harmful information impacts the security and dignity of people affected by conflict and violence, or

the ability of humanitarian actors to assist and protect them. What becomes increasingly clear, however, is that the rapid evolution and increasing use of digital information technologies is turning misinformation, disinformation, and hate speech into an exacerbating and accelerating driver of conflict dynamics, violence, and with direct and concrete harm to civilians.

Disinformation campaigns, or "psychological warfare", have long been part of armed conflicts. Hate speech has instigated the slaughter of civilians before social media existed – for example the atrocities incited by Radio Télévision Libre des Milles Collines in Rwanda in 1994. The digitalisation of societies and information technologies have brought new dimensions to the spread of harmful information: the speed of the dissemination and their capacity to reach multiple and large audiences who consume, relay and react, generating further (unverified) information – with Ukraine, Myanmar, and Sri Lanka among recent cases in point. Contexts affected by armed conflict and violence appear to be particularly vulnerable to negative impacts of harmful information. Our experience shows that misinformation, disinformation, and hate speech can contribute to psychological and social harm through online or offline harassment, defamation, and intimidation – which, in turn, can lead to physical violence, persecution, discrimination, or displacement.

> **To protect people affected by armed conflict against harmful cyber operations, concrete legal and policy steps are needed to bridge gaps between theory and practice, between battle-proven rules and new realities.**

Truth has long been seen as one of the first victims of war. Today, truth and trust in societies are primary targets of information operations. Digital mis- and disinformation indeed often target the trust people have in institutions, such as governments, sciences, media – as recently seen in the 'infodemic' linked to the COVID-19 pandemic. Such operations also harm humanitarian organisations. Their capacity to operate and serve the most vulnerable depends on trust from affected people, and trust from warring parties to be able to deploy their neutral, impartial, and independent humanitarian activities. Yet, our own operations have repeatedly been put at risk by mis- and disinformation used to jeopardise their acceptance and therefore our access to places and people in need. False and manipulated information can cause reputational damage, erode trust, and undermine communities' acceptance of humanitarian organisations.

The information landscape is constantly evolving and increasing automation or "deep fakes" will likely aggravate some of the concerns we see. To start turning the tide on the human cost of harmful information, we call for the following:

- Academia, tech companies, states, and humanitarians should work together to better understand the impact of misinformation, disinformation, and hate speech in contexts affected by armed conflict and violence, and to identify ways to address it.

- An inclusive approach is necessary. Technological advances are often driven by companies based in a few states – we need to ensure that needs of, and impact on, all people are taken into account in these processes.

Maintaining a trusted and confidential humanitarian space

Data breaches and various forms of espionage are, unfortunately, widespread. If targeted at humanitarian organisations, however, these operations risk causing severe consequences for affected people. Concretely, the data breach against the Red Cross and Red Crescent Movement included personal data such as names, locations, and contact information of missing people and their families, unaccompanied or separated children, detainees, and other people

receiving humanitarian services as a result of armed conflict, natural disasters, or migration. If in the wrong hands, the stolen data could potentially be used by states, non-state groups, or individuals to contact or find people to cause them harm, ranging from the arrest or targeting of opponents to the trafficking of unaccompanied children. Moreover, the breach forced us to take the compromised data hosting systems temporarily offline, limiting our family reunification services. In recent years, every day the Red Cross and Red Crescent Movement has helped reunite 12 people with their families – every day that these activities are disrupted continues the distress of children, women, and men.

The services of the ICRC, the wider Red Cross and Red Crescent Movement, and of other humanitarian organisations are requested by people and accepted by parties to armed conflicts in all parts of the world. The Geneva Conventions and the Movement Statutes – which are agreed to by states – mandate the ICRC to help search for missing persons, visit detainees, and reconnect family members separated by armed conflict and violence. Conducting cyber operations against humanitarian organisations or tolerating such operations undermines international humanitarian law and is irreconcilable with the widely recognised need of humanitarian relief of the most vulnerable. Humanitarian activities must be respected and protected – they are an essential contribution to help break the spiral of never-ending conflicts, reduce hatred, enhance the resilience of people and communities, and build lasting peace.

For several years, the ICRC and the Red Cross and Red Crescent Movement have warned about the critical importance and urgency for states and other actors to protect essential data and digital infrastructure from cyberattacks, intrusion, and misuse. Once we have taken all feasible steps to protect the people whose personal data has been accessed, and to restore our systems and services, data breaches of this kind will be the starting point of much-needed policy debates.

The way forward

- In the short term, states should assert in unequivocal terms that cyber operations and attacks against humanitarian organisations and data entrusted to them are dangerous and unacceptable. We also need a conversation and commitments to ensure that the international legal and policy framework adequately protects humanitarian organisations, including their data, against cyber operations;
- The humanitarian community needs to work together – and find partners – to ensure the best possible protection against cyber operations targeting humanitarian operations and personal data entrusted to us. We cannot do this alone. We need the help of tech companies, academia, and other experts, and the necessary funds to do so.
- And we will also need innovation to strengthen the protection of our systems and to foster acceptance that digital operations of humanitarian organisations are not a target – just as their physical operations. For example, the ICRC is partnering with research institutions and a global group of experts to explore the idea of a "digital emblem" to identify the data and digital infrastructure of authorised humanitarian and medical entities and to signal their legal protection – just as the universally known red cross, red crescent, or red crystal emblems do in the physical world.

It is our collective responsibility to ensure that the digital transformation of societies continues to yield societal, health, and humanitarian benefits. Unfortunately, the use of new technologies in contexts affected by armed conflict and violence also poses new risks – to humans, to critical infrastructure, to the trust that underlies life in society and to humanitarian operations. We must not forget that while digital technologies rely on, and operate in, computer systems, our focus should always be on people, especially the most vulnerable ones.

To mitigate the risks that new digital technologies pose to those affected by armed conflict and violence, states should;
- Ensure that the long-standing rules of international humanitarian law are applied in a manner that provides adequate and sufficient protection for civilians and civilian infrastructure, ICT systems, and data in our ever-increasingly digitalised societies; and
- Work on concrete actions with all relevant stakeholders – including industry, donors, civil society, media companies, NGOs – to identify concrete and comprehensive solutions to mitigate the risks to people posed by the digitalisation of armed conflicts.

ABOUT THE AUTHOR

Peter Maurer

Peter Maurer is the President of the International Committee of the Red Cross (appointed in 2012). As ICRC President he has a unique exposure to today's main armed conflicts and the challenges of assisting and protecting people in need. He travels regularly to the major conflict theatres of the world including Syria, Yemen, and the Sahel region. As the ICRC's chief diplomat, and through the ICRC's principled, neutral approach, Mr Maurer regularly meets with heads of states and other high-level officials as well as parties to conflict, to find solutions to pressing humanitarian concerns.

Mr Maurer has served as Secretary of State for Foreign Affairs in Switzerland as well as the Ambassador and Permanent Representative of Switzerland to the United Nations in New York. As a diplomat he worked on issues relating to human security, including mine action, small arms, and light weapons as well as on the responsibility of states in the implementation of international humanitarian law.

@PMaurerICRC

The **Centre for Security, Diplomacy and Strategy (CSDS)** seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy.

The **CSDS Policy Brief** offers a peer-reviewed, interdisciplinary platform for critical analysis, information and interaction. In providing concise and to the point information, it serves as a reference point for policy makers in discussing geo-political, geo-economic and security issues of relevance for Europe. Subscribe here. The CSDS Policy Brief is a discussion forum; authors express their own views. If you consider contributing, contact the editor Prof. Michael Reiterer: michael.reiterer@vub.be.

Follow us at:
Twitter @CSDS_Brussels LinkedIn CSDS Brussels Youtube CSDS
http://csds.brussels-school.be

BRUSSELS SCHOOL OF GOVERNANCE

The Brussels School of Governance is an alliance between the Institute for European Studies (Vrije Universiteit Brussel) and Vesalius College.

Visitor's address:
Pleinlaan 5, 1050 Brussels, Belgium
Mailing address:
Pleinlaan 2, 1050 Brussels, Belgium

info_bsog@vub.be

www.brussels-school.be