International Review of the Red Cross (2020), **102** (913), 367–387.
Digital technologies and war
doi:10.1017/S1816383121000151

IRRC

Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation

Massimo Marelli*
Massimo Marelli is Head of the Data Protection Office at the International Committee of the Red Cross

Abstract

Digitalization and new technologies have an increasingly important role in today's humanitarian activities. As humanitarian organizations become more active in and reliant on new and digital technologies, they evolve from being simple bystanders to being fully fledged stakeholders in cyberspace, vulnerable to adverse cyber operations that could impact on their capacity to protect and assist people affected by armed conflict or other situations of violence.

* The opinions and views expressed in this article are the author's own and do not necessarily represent those of the ICRC. The author is grateful to Bruno Demeyere, Kubo Mačák, Tilman Rodenhäuser, Andrea Raab, Eve La Haye, Gilles Cerutti, Delphine Van Solinge, Pierrick Devidal, Vincent Graf Narbel, Fabien Leimgruber, Martin Schuepp, Adrian Perrig, Sai Sathyanarayanan Venkatesh and Saman Rejali for their valuable feedback on an earlier draft. All errors are the author's own.

This shift makes it essential for humanitarian organizations to understand and properly map their resulting cyber perimeter. Humanitarian organizations can protect themselves and their activities by devising appropriate cyber strategies for the digital environment. Clearly defining the digital boundaries within which they carry out operations lays the groundwork for humanitarian organizations to develop a strategy to support and protect humanitarian action in the digital environment, channel available resources to where they are most needed, and understand the areas in which their operational dialogue and working modalities need to be adapted for cyberspace.

The purpose of this article is to identify the unique problems facing international humanitarian organizations operating in cyberspace and to suggest ways to address them. More specifically, the article identifies the key elements that an international humanitarian organization should consider in developing a cyber security strategy. Throughout, the International Committee of the Red Cross and its specificities are used as an example to illustrate the problems identified and the possible ways to address them.

Keywords: cyber, cyber strategy, cyber security, cyber operations, cyber attack, digital services, international organizations, humanitarian organizations, humanitarian action, digital transformation.

Introduction and "setting the scene"

Digitalization and new technologies have an increasingly important role in today's humanitarian activities.[1] This is happening for a number of reasons and in response to a number of new challenges. For example, armed conflicts are more and more fragmented and difficult to read, and security and acceptance are more and more fragile, making it harder for international humanitarian organizations[2] to access conflict areas and affected people.

Some of the topics considered in this article first appeared as part of a series of blog articles on the ICRC's *Humanitarian Law and Policy Blog*: see Massimo Marelli, "Hacking Humanitarians: Moving Towards a Human Cybersecurity Strategy", 16 January 2020, available at: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/; Massimo Marelli and Adrian Perrig, "Hacking Humanitarians: Mapping the Cyber Environment and Threat Landscape", 7 May 2020, available at: https://blogs.icrc.org/law-and-policy/2020/05/07/hacking-humanitarians-mapping-cyber-environment/; Massimo Marelli and Martin Schüepp, "Hacking Humanitarians: Operational Dialogue and Cyberspace", 4 June 2020, available at: https://blogs.icrc.org/law-and-policy/2020/06/04/hacking-humanitarians-dialogue-cyberspace/.

1 See Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector", *Humanitarian Law and Policy Blog*, 5 December 2016, available at: https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/ (all internet references were accessed in January 2021).

2 This article's scope of analysis is restricted to international humanitarian organizations – i.e., organizations that have international organization or equivalent status and that have a humanitarian mandate. This does not include non-governmental organizations. The major difference between international humanitarian organizations and non-governmental organizations, for the purposes of this

It is against this backdrop that humanitarian organizations have strived to evolve and adapt in order to be better able to respond to humanitarian crises. They have started looking with interest at the possibility of complementing physical proximity with digital proximity – for example, by being accessible and responding to requests for information and assistance through social media or messaging apps.[3] They are developing new digital channels to deliver existing humanitarian services as well as new, natively digital services to affected populations that might already access other public and private services online and might expect the same of humanitarian organizations. They also see the positive role of digital platforms in consolidating existing resilience mechanisms of affected populations or enabling new ones, and are asking themselves how they can play a role in facilitating or enhancing such resilience mechanisms.[4]

Moreover, an increasing number of armed conflicts and other situations of violence are taking place in urban, connected environments[5] where it is often not the lack of data that makes it difficult to get proper situational awareness, but, rather, the abundance thereof and the difficulty in making sense of it. Humanitarian organizations are therefore considering the advantages of using new technologies, such as artificial intelligence (AI), machine learning and big data, to try and make sense of the complex environments in which they need to operate.[6] These technologies are sometimes built into commercially available products which can be acquired off the shelf from companies that are often interested in partnering with humanitarian organizations.

In addition, armed conflicts are lasting longer. The average length of time that the International Committee of the Red Cross (ICRC) has been present in the countries hosting its ten largest operations is more than forty years.[7] In protracted conflicts, humanitarian action may be required to plan for a long-term response that goes well beyond immediate and one-off distribution of food and non-food items or war surgery, and encompasses repeat distributions of aid in the long term. This

analysis, is the extent to which an international humanitarian organization enjoys privileges and immunities to ensure that it can perform its mandate in full independence. The existence and work of international humanitarian organizations is central to the functioning of the international community, and the international community relies on international humanitarian organizations to take care of tasks which individual States or groups of States cannot achieve alone. This makes international humanitarian organizations very relevant, but at the same time, potentially very vulnerable as cyber targets. However, the specific status they enjoy, and their privileges and immunities, can provide important safeguards for the protection of the organization if properly applied in a cyber environment.

3 See International Committee of the Red Cross (ICRC), in collaboration with The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action*, January 2017, available at: www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

4 See A. Kaspersen and C. Lindsey-Curtet, above note 1.

5 See David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*, Oxford University Press, Oxford, 2015, available at: www.kilcullenstrategic.com/out-of-the-mountains/.

6 See Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of the Red Cross*, Vol. 99, No. 904, 2017.

7 See Ellen Policinski and Jovana Kuzmanovic, "Protracted Conflicts: The Enduring Legacy of Endless War", *International Review of the Red Cross*, Vol. 101, No. 912, 2019, p. 965.

response also includes working on systems and infrastructure such as water, sanitation and electricity. In this context, digital identification of beneficiaries – including, to some extent, biometric technology – becomes of interest for the humanitarian sector.

This process of "digital transformation", with humanitarian services being offered and made accessible digitally, is taking the collection and generation of personal data to a new scale. When combined with the introduction of commercial and/or technical third-party stakeholders, which are usually necessary to deliver relevant services digitally, it becomes a paradigm shift in the dynamics of humanitarian action delivery which organizations must take into account in relation to their bilateral interactions between humanitarian actors and their interlocutors. This shift brings into the picture technology providers, financial institutions, mobile network operators, and stakeholders involved in large-scale mass surveillance of telecommunications networks or targeted digital surveillance.

Personal data protection is an essential tool to enable humanitarian organizations to fully understand and dissect data flows, identify external stakeholders, map new risks and help identify mitigating measures. Therefore, it is crucial to enable the adoption of new technologies in a way that respects the rights, dignity and agency of affected populations and ensures accountability of and trust for humanitarian organizations, as well as upholding the responsibility to "do no harm" in the digital environment.[8]

As a consequence, data protection and ethics are key elements informing how an organization shapes the ways in which it carries out its work in favour of affected people in cyberspace, and therefore, its cyber perimeter. However, this analysis aims to go beyond strictly exploring the personal data protection aspects of digital transformation and humanitarian data ethics. Rather, it aims to unpack the unique problems faced by international humanitarian organizations operating in cyberspace and to propose solutions to address them. More specifically, the article intends to look at how the combination of an increased digital footprint, on the one hand, and the legal, technical and geopolitical implications of digitalization in the humanitarian sector, on the other, shape the cyber perimeter of an international humanitarian organization. For the purposes of this article, the cyber perimeter of an organization is defined as all the elements that jointly shape the presence and behaviour of the organization in cyberspace: its mandate, the activities it carries out in cyberspace, and how it goes about implementing

8 On data protection in humanitarian action, see Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC, Geneva, 2020, available at: https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-print-en. On the implications of metadata generation through third-party interactions in delivering humanitarian programmes, see Tina Bouffet and Massimo Marelli, "The Price of Virtual Proximity: How Humanitarian Organizations' Digital Trails can Put People at Risk", *Humanitarian Law and Policy Blog*, 7 December 2018, available at: https://blogs.icrc.org/law-and-policy/2018/12/07/price-virtual-proximity-how-humanitarian-organizations-digital-trails-put-people-risk/. On of the use of biometric data by the ICRC, see Ben Hayes and Massimo Marelli, "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy", *Humanitarian Law and Policy Blog*, 18 October 2019, available at: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.

and protecting those activities, particularly in anticipation of and in response to specific threats.

Understanding and conceptualizing their cyber perimeter is essential for organizations working in humanitarian action and undergoing a process of digital transformation of the magnitude mentioned above. As these entities become more active in and reliant on cyberspace, they are moving away from being bystanders and towards being fully fledged stakeholders in this domain, itself vulnerable to adverse cyber operations, or to being caught up in "cross-fire", which might impact their capacity to carry out humanitarian activities for those most in need.

This shift makes it essential for humanitarian organizations to understand and properly map their resulting cyber perimeter. Doing this effectively can allow them to delineate a strategy to support and adequately protect the delivery of humanitarian action in the digital environment; to channel the resources available to where they are most needed; and to understand the areas in which their operational dialogue and working modalities need to be adapted to be fit for cyberspace.

In this sense, an international humanitarian organization's cyber perimeter may be analyzed in light of: (1) what the organization wants to do in the digital environment and the organization's digital humanitarian operations; (2) the identity, mandate and *modus operandi* of the organization, and the affected people it serves; and (3) the cyber environment, particularly regarding the challenges and threats that the organization faces in the digital space.

This paper argues that these aspects, and the challenges arising under each of them due to the organization being active in cyberspace, should shape an organization's cyber security strategy. Such a strategy would thereby set out the following (non-exhaustive) protections and affiliations: (1) the legal protections it needs to seek; (2) the technical protections it is entitled to or can seek for its data and for its data flows; and (3) the stakeholders it needs to engage with and the operational dialogue it deploys with them. Each of these elements is analyzed, in turn, below.

What the organization wants to do in the digital environment, and the organization's digital humanitarian operations

To accurately determine an organization's cyber perimeter, the first step is to analyze precisely what it is that the organization wants to do in cyberspace, and to map the organization's current or envisaged digital humanitarian operations. This will be essential to determining the other elements of the organization's cyber perimeter and what the organization can do to secure it, as will be seen further below.

In the case of the ICRC, offering digital services directly to beneficiaries is at the core of this organization's institutional strategy for 2019–22.[9] This strategy is

9 See ICRC, *ICRC Strategy 2019–2022*, Geneva, September 2018, available at: www.icrc.org/en/publication/4354-icrc-strategy-2019-2022.

dictated primarily by (1) the increased challenges in having physical access to conflict areas, and the consequent need to complement physical proximity with digital proximity and accessibility; and (2) the fact that conflicts increasingly take place in areas where people are more likely to have access to connectivity, are used to accessing services online, and expect to interact with humanitarian organizations digitally. This reality requires the ICRC to engage in significant digital transformations in order to meet its objectives. This, in turn, will lead the organization to exponentially increase its digital footprint, and this is a trend that is common to most organizations, both in the humanitarian sector and beyond, in the digital era. This trend is one that comes with a natural increase in attack surface and exposure, and attractiveness as a target of adverse cyber operations.[10]

An important objective of the ICRC is linked to leveraging data (both data generated as part of its digital growth and data generated, acquired or available externally) by, for example, enabling predictive analytics and big data analysis, or developing or fine-tuning AI and machine learning tools to help solve problems that are specific to humanitarian action. This is important as it may help to inform the organization's decisions and improve its operational readings of armed conflicts and other situations of violence – for example, by informing its readings of anticipated displacement patterns, identifying influencers within parties to a conflict that can be relevant interlocutors to ensure access, or improving logistics and supply chain management.[11] Leveraging data can also be useful to support humanitarian action through various data science tools and techniques, from statistics to AI (for example, by using facial recognition for the determination of the whereabouts of missing persons).[12]

Thus, in the case of the ICRC, the organization wants to use the cyberspace domain to (1) achieve digital proximity to complement physical proximity, offering humanitarian services and being reachable digitally and remotely by affected populations that are increasingly connected; (2) facilitate and leverage new resilience mechanisms of affected populations enabled by digital platforms; and (3) leverage data to better inform its decision-making, which then feeds into how its cyber perimeter will be shaped.

The organization's identity, mandate and *modus operandi*

To determine an organization's cyber perimeter, it is important to place the organization's identity, mandate and *modus operandi* at the centre of the analysis, in order to determine what needs to be protected and how it can be protected

10 See ICRC, *The Potential Human Cost of Cyber Operations*, Geneva, 29 May 2019, available at: www.icrc.org/en/document/potential-human-cost-cyber-operations.

11 See, for example, "Big Data, Migration and Human Mobility", *Migration Data Portal*, available at: https://migrationdataportal.org/themes/big-data-migration-and-human-mobility.

12 See, for example, ICRC, "Rewards and Risks in Humanitarian AI: An Example", *Inspired*, 6 September 2019, available at: https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/.

with respect to the cyberspace domain. Each organization should start its analysis from the specificities of the organization.

Taking again the example of the ICRC, this organization is a neutral, impartial, independent organization with the exclusively humanitarian mission to protect the life and dignity of victims of armed conflicts and other situations of violence. The work of the ICRC is based on the Geneva Conventions of 1949, their Additional Protocols, the organization's Statutes and those of the International Red Cross and Red Crescent Movement (the Movement), and the resolutions of the International Conferences of the Red Cross and Red Crescent.

The ICRC enjoys a special legal status and privileges and immunities under both international and domestic law.[13] The purpose of the privileges and immunities is to enable the ICRC to effectively carry out its mandate, and to do so in full conformity with its Fundamental Principles and standard working modalities.[14]

As will be seen further below, the ICRC's neutrality, impartiality and independence, the exclusively humanitarian nature of its work, and the privileges and immunities it enjoys in most of the countries in which it operates, enable it to carry out its mandate and are all essential elements shaping the organization's cyber perimeter and clearly distinguishing it from the cyber perimeters of other organizations.

The ICRC is entrusted by governments, through international humanitarian law and the Statutes of the Movement,[15] to assist and protect people during armed conflict and other situations of violence. To be able to carry out this mandate today, as outlined above, the organization also needs to be present and act in cyberspace by, for example, providing digital services. The same commitment from governments that would apply in the physical world to respect the ICRC's work as well as its working modalities for the benefit of populations affected by armed conflicts and other situations of violence should apply, *mutatis mutandis*, in cyberspace.

In carrying out its mandate, the ICRC adopts a proximity-based approach, through its approximately 20,000 staff members across eighty countries, in order to respond to the humanitarian needs of affected populations and to engage with key stakeholders on the application of international humanitarian law.[16] Unlike other humanitarian organizations that often operate through implementing partners, the ICRC's type of work requires direct proximity with affected populations (e.g. displaced populations, people deprived of their liberty, the wounded and sick, separated family members and unaccompanied minors, and families of the

13 See Els Debuf, "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897/898, 2016, available at: https://international-review.icrc.org/articles/tools-do-job-icrcs-legal-status-privileges-and-immunities.

14 See ICRC, "Fundamental Principles", available at: www.icrc.org/en/fundamental-principles.

15 See Statutes of the International Red Cross and Red Crescent Movement, adopted by the 25th International Conference of the Red Cross, Geneva, 1986 (amended 1995, 2006), available at: www.icrc.org/en/doc/resources/documents/misc/statutes-movement-220506.htm.

16 See ICRC, "What We Do", available at: www.icrc.org/en/what-we-do.

missing) as well as a physical presence in the areas where those affected populations are located.

An essential precondition for access is trust. This relates to the trust of both (1) affected populations and (2) parties to the armed conflict and actors in other situations of violence. As far as affected populations are concerned, trust is established by the guarantee that any engagement between them and the ICRC will be exclusively humanitarian. In particular, affected people expect that the information they provide for exclusively humanitarian purposes is treated as such and is not used or handled in a way that is detrimental to their safety or to humanitarian action more generally, such as when non-humanitarian stakeholders use the information for the furtherance of conflict-related objectives, counterterrorism agendas, migration flow controls or commercial exploitation. The importance of ensuring that data collected for humanitarian purposes are not used for other purposes is acknowledged in both the Resolution on Privacy and International Humanitarian Action (adopted by the International Conference of Privacy and Data Protection Commissioners in Amsterdam in 2015)[17] and the Movement's 2019 resolution on "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection".[18]

As far as parties to an armed conflict and actors in other situations of violence are concerned, to establish trust, they need to be confident that the work of the organization is neutral, impartial, independent and exclusively humanitarian. This entails that the organization take measures to minimize the risk that the data it collects will be accessed by such actors and to ensure that it does not end up being used to further conflict-related purposes, used by law enforcement or intelligence agencies, used as evidence in criminal proceedings, or otherwise made public. One of the key working modalities enabling the ICRC to have access to conflict areas and people affected by conflict is, therefore, that of confidentiality.[19] In particular, the ICRC does not share with any third parties information relating to its confidential bilateral dialogue with the authorities and other actors involved in conflicts and other situations of violence. This working modality is also safeguarded by the privilege of non-disclosure, a specific protection under customary international law from which the ICRC is the only organization to benefit.[20]

Although no academic study appears to be available to support this finding, it is the experience of the author and other humanitarian operators that in the

17 See "Resolution on Privacy and International Humanitarian Action", 37th International Conference of Data Protection and Privacy Commissioners, Amsterdam, 27 October 2015, available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

18 See ICRC, "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection", 33IC/19/R4, Resolution 4 adopted at the 33rd International Conference of the Red Cross and Red Crescent, Geneva, 9–12 December 2019, available at: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

19 See ICRC, "Confidentiality Q&A", 15 January 2018, available at: www.icrc.org/en/document/confidentiality-q.

20 See E. Debuf, above note 13.

physical world, and to achieve physical proximity, trust is gained through a number of factors, including vulnerability.[21] In order to ensure and secure its presence, the ICRC does not generally rely on armed escorts and armoured vehicles, or on physical barriers; rather, and with all the vulnerability that this involves, it relies only on the acceptance of its humanitarian work and trust in its neutral, impartial and independent approach. If a stakeholder is not convinced about this, the organization's staff and assets would be very easy to target. The fact that the organization and its staff expose themselves and are so vulnerable vis-à-vis any possible ill-intentioned third parties leads interlocutors to trust that the organization stands for what it says and does not have ulterior motives.

In the digital world, however, vulnerability is not a strength but a weakness. The idea that the systems of the organization could easily be breached if anyone wanted to attack them would, alone, destroy any trust in the organization and discourage stakeholders from engaging with it. Therefore, to establish trust, to ensure digital proximity and to avoid causing detriment to physical proximity, the ICRC must be able to demonstrate the security and resilience of its cyber infrastructure. It is therefore essential for an international humanitarian organization to have full awareness of its cyber environment, challenges and threats.

The cyber environment, and the challenges and threats an organization faces therein

The cyber environment in which an international humanitarian organization operates presents a number of threats. These are often analyzed through the "confidentiality, integrity, availability" (CIA) triad.[22] As discussed below, in the case of international humanitarian organizations, the "classic" CIA analysis is not sufficient and needs to be adapted to take into account specific security threats arising from "jurisdictional" considerations – i.e., the fact that access may take place by virtue of authorities exercising jurisdiction over processors or sub-processors. Additional and specific considerations should be developed concerning the security of the supply chain. Each of these aspects is analyzed, in turn, below.

Confidentiality

A humanitarian organization may have to deal with situations in which individuals or groups supporting one party to an armed conflict (or actor in other situations of violence) may try to access sensitive data held by the organization. This is because the data in question may relate to specific individuals of interest, or populations

21 See Philippe Dind, "Security in ICRC Field Operations", *Secure 02*, Finnish Red Cross, June 2002, p. 27, available at: www.icrc.org/en/doc/assets/files/other/secure02_dind.pdf.

22 See Michael Nieles, Kelley Dempsey and Victoria Yan Pilliterri, *An Introduction to Information Security*, NIST Special Publication 800-12, National Institute of Standards and Technology, June 2017, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

linked to or of the same ethnic origin or national or political affiliation as that party's enemy. Health information, for example, may indicate a medical condition that is linked to a high-value target.[23]

"Big data theft" attacks are also a possible, important, confidentiality-type challenge. These may be aimed at collecting as many large data sets as possible, which are then correlated, analyzed, and used to profile individuals of interest to the attacker.[24] Such individuals might include beneficiaries of humanitarian action or other interlocutors of the humanitarian organization's neutral and impartial dialogue. Individuals so profiled could then be put under targeted surveillance, and data about them possibly used to inform additional actions in furtherance of conflict-related objectives. This concern may relate to large data sets, including metadata (that is, data about data), held both by humanitarian organizations themselves and by their third-party service providers (such as telephone companies or financial institutions), which may generate and use these data in the framework of humanitarian programmes such as mobile cash transfers.

Collaboration with or engagement of third-party technology service providers to handle or process data, such as through certain types of cloud-based solutions or in cash transfer programmes involving financial service providers and/or mobile network operators, is also extremely significant for the discussion on confidentiality. International humanitarian organizations can benefit from certain privileges and immunities regarding the data they collect. Where they do, the authorities cannot lawfully use due process to seek to access data they hold, thereby preserving confidentiality. It is very important that similar protections are acknowledged where it is a third-party service provider that processes data for the organization, though specific challenges involved in the generation and processing of data by third-party providers through digital tools make this principle difficult to apply.

To understand how third-party service providers can pose a threat to the data security of an international humanitarian organization, it is necessary to have a clear appreciation of the application of the principle of sovereignty to cyberspace, in particular by analyzing how States see their jurisdiction over technology providers, the infrastructure that supports data flows, and the data flows themselves, whether on their territory or outside. It is key for an international humanitarian organization, and particularly one like the ICRC, to ensure that no authority can by due process legitimately seek access to data held by the organization, whether directly or through third-party processors.

A digitalization of the scale and magnitude highlighted above, however, is most likely not going to be possible without leveraging the public cloud for at least

23 See, for example, C. Currier, "The NSA Plan to Find Osama Bin Laden by Hiding Tracking Devices in Medical Supplies", *The Intercept*, 21 May 2015, available at: https://theintercept.com/2015/05/21/nsa-plan-find-osama-bin-laden-infiltrating-medical-supply-chain/.

24 See, for example, Bill Gertz, "Cybercom: Big Data Theft at OPM, Private Networks Is New Trend in Cyber-Attacks", *Washington Free Beacon*, 27 July 2015, available at: https://freebeacon.com/national-security/cybercom-big-data-theft-at-opm-private-networks-is-new-trend-in-cyber-attacks/.

part of the organization's service offering.[25] Technology companies are increasingly and rapidly pushing their offering of software and storage to the public cloud and are no longer supporting non-cloud-based alternatives, often rendering them obsolete. In addition, certain tools enabling maximization of information – through, for example, AI – may be procured and deployed more efficiently on the public cloud. Because of this, the non-cloud-based model involving solutions held, managed and supported on the premises of the organization, traditionally favoured by security-conscious organizations, is harder and harder to sustain over the medium term. Even software that is procured as an on-premise solution today is likely to be linked to public cloud applications and/or sharing diagnostic or telemetry data across jurisdictions.[26] This means that data collected and generated by an organization will most likely be processed by third-party technology providers at some point. This brings significant new challenges in guaranteeing confidentiality.

It is therefore important for humanitarian organizations to carefully analyze this area and find solutions that are suitable for the sensitive work they are doing. Such considerations ought to bear in mind the specific architectural features of the public cloud[27] and legislation allowing authorities to access data generated and/or stored outside of their territory, such as the US CLOUD Act and other equivalent legislation elsewhere. CLOUD Act-type legislation and its impacts are spreading fast around the world,[28] due primarily to two factors: (1) other countries replicating the Act in order to assert jurisdictional control over data, and (2) agreements between the United States and third countries, under the CLOUD Act itself, allowing both parties to seek access to data under one another's jurisdictional control.

Integrity

From the point of view of integrity, an important challenge comes from the increasing use of AI and machine learning in supporting decision-making and situational awareness. This situation raises the threat that third parties might tamper with the accuracy and integrity of data used to train algorithms and develop models, as well as data sets used for the analysis, thereby interfering with the outcome of the analysis and decision-making.[29] Humanitarian organizations may, consequently, be manipulated into wrongly prioritizing certain affected populations over others or operating in particular areas over others, or be

25 For a description of the public cloud and why it can be an important asset to leverage, see Microsoft, "What Are Public, Private, and Hybrid Clouds?", available at: https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

26 See, for example, Dutch Ministry of Justice, *DPIA Office 365 ProPlus Version 1905: Data Protection Impact Assessment on the Processing of Diagnostic Data*, June 2019, available at: www.government.nl/documents/publications/2019/07/22/dpia-office-365-proplus-version-1905.

27 See Microsoft, "What Is Cloud Computing? A Beginner's Guide", available at: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/.

28 See US Department of Justice (DoJ), "CLOUD Act Resources", available at: www.justice.gov/dag/cloudact.

29 See C. Kuner and M. Marelli (eds), above note 8, Chap. 16.3.5.

otherwise manipulated in ways that may be detrimental to affected populations, or to the neutrality, impartiality and independence of their action.

Availability

From the point of view of availability, or ensuring timely and reliable access to and use of information, the concern is with situations in which the humanitarian organization offers digital services to affected populations. This can happen in a situation in which digital proximity is successfully deployed to complement physical proximity, or in a situation in which physical access is impossible and digital access is used instead. If affected populations rely on the availability of digital services from humanitarian organizations for their livelihood or for humanitarian protection, any cyber operation affecting availability of these services will have humanitarian consequences. In these cases, cyber operations affecting the availability of (digital) humanitarian services, like distributed denial-of-service (DDoS) operations or operations involving ransomware, raise very serious humanitarian concerns. Within this category, humanitarian organizations should also consider the implications for their capacity to deliver digital humanitarian services and for the possibility for affected populations to access them.[30] In addition, although not directly a type of challenge affecting the systems and infrastructure of an organization, humanitarian organizations also need to consider in their cyber perimeter the possibility that operations may be carried out by a stakeholder that would use cyber means against its adversaries by impersonating the organization or exploiting its name[31] or reputation, thereby attacking the sense of trust that individuals may have in it.

Supply chain security

Specific challenges are presented in ensuring the security of the supply chain.[32] This means, for example, that no back doors are present in the hardware or software procured and used by the humanitarian organization to deliver digital humanitarian services and/or to operate its systems. As far as hardware is concerned, while it may be possible for an organization, going forward, to effectively invest in the security of some key components of the hardware it procures,[33] it will still be unrealistic to aim for security of all the components it requires.

30 See Berhan Taye and Sage Cheng, "The State of Internet Shutdowns", *Access Now*, 8 July 2019, available at: www.accessnow.org/the-state-of-internet-shutdowns-in-2018/.

31 See, for example, Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender", *Citizen Lab*, 24 August 2016, available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

32 See, for example, ICT Switzerland, "Supply Chain Security", available at: https://ictswitzerland.ch/en/topics/cyber-security/supply-chain/.

33 See Fabio Bergamin, "Open-Source Microprocessor", *ETH Zürich*, 30 March 2016, available at: https://ethz.ch/en/news-and-events/eth-news/news/2016/03/open-source-microprocessor.html.

A comprehensive strategy to address supply chain security concerns may need to be developed by the organization. Such a strategy would need to cover a combination of elements such as open-source hardware components, procurement practices, usage awareness and practices (such as staff training, but also minimizing the capacity of the hardware and software so that they process only the data and perform only the operations that are strictly required for the purposes of the processing), and partnerships with academia on solutions to monitor performance of hardware in order to detect possible anomalies linked to a compromised piece of hardware.[34] As far as software is concerned, some software companies may provide access to source code to countries and international organizations so that they can audit it and verify that no back doors are present.[35]

Although an international organization may seek access to such programmes, this may not be a solution available with all suppliers. In addition, even if the organization did have access to the source code, it may not have the means to effectively review all the lines of code of the software procured and thereby ensure its own protection.

The legal protections that an international humanitarian organization needs to seek

The first countries to explore the legal implications of hosting data for another subject of public international law were the governments of Estonia and Luxembourg, with the establishment of Estonia's "data embassy" in Luxembourg in 2017.[36] The interpretation of the law in this area is not fully settled, and in this section of the article, a number of unanswered questions are raised along with recommendations for possible clarifications that can be sought in relation to privileges and immunities to ensure that headquarters agreements fully reflect the specific needs raised by the hosting of data and applications in the strategic locations where the organization bases the most significant hosting of its data and applications.

The independence required by an international organization to fully and effectively implement its mandate is generally safeguarded in headquarters, status or host-State agreements. These provide for a series of privileges and immunities for the organization and its staff, including immunity from judicial or administrative process for the organization and its property, assets and staff, as well as inviolability of its premises, property, assets, correspondence and archives.

34 See Markus Gross, "A Booting Computer Is as Vulnerable as a Newborn Baby", *ETH Zürich*, 5 November 2019, available at: https://ethz.ch/en/news-and-events/eth-news/news/2019/11/project-opentitan.html.

35 See Microsoft, "Government Security Program", available at: www.microsoft.com/en-us/securityengineering/gsp.

36 See e-Estonia, "Estonia to Open the World's First Data Embassy in Luxembourg", available at: https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

Clarifications may be required as to the interpretation of these agreements and their application in the digital environment.

It is important to clarify the application of the privileges and immunities of international organizations to include data (in transit, at rest and in processing) stored and processed not only by the humanitarian organization directly, but also by third-party service provider(s) or separate organization(s), including when hosted or otherwise processed by third-party technology providers on behalf of the organization, as well as the servers and networks used by the organization, whether they belong to the organization or to a third-party service provider.[37] Surprisingly, and to the best of this author's knowledge, no literature exists on this very important question.

Other provisions typically found in headquarters agreements generally involve guarantees that the host State will permit the organization's free use of the means of communication that the organization deems most appropriate, for official purposes and without any interference. Data flows required for and generated by the deployment of digital humanitarian services are covered by these guarantees, in addition to immunity and inviolability provisions. The agreements also cover the freedom for the organization to deploy specific technical protections in order to give practical effect to these provisions. Such protections could include sophisticated encryption algorithms or technologies incorporating them, and technologies aimed at preventing interference with, or interception of, communications and data flows involving the organization.

The agreement between an international humanitarian organization and a host State may also need to clarify that permitting and protecting free use of the means of communication includes, for instance, not interfering with access to the Internet and not interrupting or slowing down the internet connection of the organization or of a third-party service provider in a targeted manner. Considering that some measures of this type may be necessary to deal with DDoS attacks, however, and to avoid unintended consequences, it would also be important to clarify how these guarantees apply in scenarios where the organization is subject to a DDoS operation. While guaranteeing free communications may require that a host State does not block or reduce data traffic to the organization, such measures may be necessary if the host State is to protect such communications in cases of DDoS operations affecting the organization.

Specific considerations may need to be taken into account in cases where the organization processes data through cloud providers established in the host State. In particular, in addition to the considerations listed above, it would be necessary to clarify whether and to what extent staff of the third-party technology provider may also be covered by the immunities of staff linked to the tasks

37 For a reference to the US State Department's position supporting such application of privileges and immunities of States, see *Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation*, 2015, p. 14, n. 12, available at: https://tinyurl.com/3rucylfy.

carried out in the performance of their functions as staff of the organization, insofar and to the extent that they process data of the organization and have access to clear, unencrypted data. These individuals may come into contact with sensitive information, for example to provide technical support or maintenance, and thus should be granted some limited functional immunity. Certain technical solutions are currently under way that could potentially address this issue;[38] some, like homomorphic encryption,[39] seem to be promising. However, their functionality, effectiveness and scalability still need to be fully tested.

In addition, due consideration may need to be given to the application of agreements for the sharing of data between the host country and third countries, as well as to the possibility that third countries may seek to access data held by technology companies through US CLOUD Act-type legislation and other relevant domestic laws having extraterritorial implications.[40]

Finally, such agreements should consider the implications of internet shutdowns for the digital operations of the organization and seek specific protections against them. The organization should, for example, seek to negotiate specific guarantees that all traffic directed to or from the humanitarian organization will not be blocked. This may not be sufficient, however, to ensure that beneficiaries can have access to humanitarian services provided by digital means in cases where entire mobile and telecommunications networks are shut down, where it is prohibited for affected populations to obtain SIM cards, or where mobile data traffic is restricted for them and where the problem is therefore not one of network traffic but one of network access. Alternative strategies will need to be developed by the organization in order to address these cases, as part of the development of the organization's cyber strategy.

In cases where the humanitarian organization processes data through third-party technology providers, such as a cloud solution provider, the organization would then need to ensure that any clarifications between itself and the host State, as highlighted above, are also reflected in the contractual arrangements with the technology company, to ensure that the company commits to defending them and the company's staff is prepared to give effect to them.

The legal measures described above are primarily aimed at ensuring an organization's independence. Indeed, safeguarding the confidentiality of an organization's data through its privileges and immunities plays an important role in ensuring that the organization can carry out its mandate effectively – and in the case of the ICRC, also in line with the Fundamental Principles of the Movement. In this sense, it is important to stress that solutions which may be described as very secure, and accepted as such in highly regulated industries characterized by high sensitivity of data and confidentiality requirements (such as the banking industry), may nonetheless be totally inadequate for use by the

38 See Microsoft, "Confidential Computing", available at: www.microsoft.com/en-us/research/theme/confidential-computing/.

39 See Andy Greenberg, "Hacker Lexicon: What Is Homomorphic Encryption?", *Wired*, 11 March 2014, available at: www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/.

40 See DoJ, above note 28.

ICRC, since such – very secure – solutions may still involve ways for organizations to be obliged to hand over data to States, may be subject to encryption back-door legal requirements, and so on.[41]

Legal protections are not enough: The technical protection a humanitarian organization is entitled to/can seek for its data, and for data flows

The legal protections described above, alone, are however insufficient to ensure that no authority can lawfully access the data of international humanitarian organizations. Three aspects are of particular concern in this sense: (1) surveillance practices are not always in line with privileges and immunities, (2) data traffic may also be caught and intercepted as part of large-scale/bulk data collection, and (3) the data of an organization may be hosted and processed through commercial technology providers.

The consequence of these issues is that an organization needs to act on two different levels. The first is the legal level, aiming to ensure that no third actor may successfully claim access to its data by application of the law; the second is the technical and organizational level, with specific measures aimed at ensuring secure data flows, hosting, and processing. As highlighted above, these measures may not, at present and for some types of cloud architectures, be available from the market, and may need to be procured as part of research and development partnerships with academia and other partners, to be then converted into sustainable solutions. Considering costs and available resources, it may be necessary for international humanitarian organizations to pool resources with other organizations with similar mandates and status, particularly to ensure the conversion into sustainable solutions of the research and development technical aspects.

The operational dialogue deployed by the organization

As highlighted in detail above, an organization like the ICRC seeks to establish its presence and work based on acceptance, and this in turn is based on the trust that derives from its neutrality, impartiality and independence, from the fact that it furthers exclusively humanitarian objectives, and from its confidential approach. In this sense, being able to establish bilateral, confidential dialogue with all stakeholders, irrespective of whether they are State or non-State actors and whether they may be accepted as lawful groups or not, is an essential requirement in order to ensure performance of the mandate.

41 See, for example, Julia Carrie Wong, "US, UK and Australia Urge Facebook to Create Backdoor Access to Encrypted Messages", *The Guardian*, 4 October 2019, available at: www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption.

These are the features that shape the dialogue which the organization, in this case the ICRC, needs to have, also in the cyber realm.

Dialogue with "cyber host States"

Developing and deploying digital humanitarian services, as discussed, requires an organization to identify one or more key jurisdictions where it can safely host such services and procure the necessary ingredients to then offer them globally. These "cyber host States" are likely to be stable countries where no active conflict or other situation of violence is present and where, therefore, the humanitarian organization would otherwise be unlikely to run any humanitarian programmes. They are likely to be identified among technologically advanced countries with a strong cyber industry, capabilities, academia and infrastructure. One example is the recently updated agreement between the ICRC and the Swiss Confederation.[42]

Operational dialogue with cyber host States is framed, first of all, in the host State agreement itself, and any further memoranda of understanding, documents, or practices existing between the two. This dialogue should be shaped as to cover, at least, the aspects set out below.

First, dialogue should address potential cooperation regarding the anticipation, detection and attribution (an essential precondition to bilateral confidential dialogue) of cyber operations, as well as the identification of the appropriate response to them. Because of its control over the network on its territory and flows of data going through it, the resources and expertise available, and the international cooperation networks it is likely to be involved in, a cyber host State may have much better means than the organization alone to anticipate, detect, attribute and respond to cyber operations. Defining the perimeters of this dialogue will be a very sensitive task and will be important in order to ensure that, on the one hand, the dialogue is effective, while, on the other hand, it does not make the organization over-reliant on the cooperation of the cyber host State, thereby creating a risk that the neutrality, impartiality and independence of the organization will be compromised.

Second, due consideration must be given to how to deal with "cyber criminals" – i.e., cases in which an operation affecting the organization is attributed to criminal groups and is not linked to State or State-sponsored actors. To what extent can or should the organization rely on law enforcement by the host State to protect its activities, and what type of cooperation does this require? How can the organization and the host State deal with the cross-border and international nature of cyber criminals, whereby the cyber criminals may not be found in the jurisdiction of the host State, and the impact of the action may reveal itself in third countries where the organization deploys its humanitarian action? What types of international cooperation mechanisms does the host State

42 ICRC and Swiss Federal Council, "Accord entre le Conseil fédéral suisse et le Comité international de la Croix-Rouge en vue de déterminer le statut juridique du Comité en Suisse", 19 March 1993, available at: www.fedlex.admin.ch/eli/cc/1993/1504_1504_1504/fr#sidebarLink.

engage in, and are these suitable for the nature, mandate and working modalities of the organization?

Third, the dialogue should also clarify how to deal with adverse cyber operations attributed to third countries, including by State-sponsored actors. This is also a sensitive area that may need to be specifically discussed and agreed between the organization and the host State, since it may raise sensitive questions of public international law and international relations. These questions may relate to the violation of sovereignty of the host State, possible countermeasures available to the host State, and reliance on due diligence obligations of third countries under international law to support bringing the adverse operation to an end, on the one hand, and the neutrality, impartiality and independence of the organization, on the other.

While some of these questions, relating in particular to a host State's failure to assist an international organization and the availability of countermeasures, have been analyzed in detail,[43] many others remain. In particular, while questions around sovereignty, countermeasures and due diligence in cyberspace have been discussed in different fora[44] and in certain governments' cyber security policies and/or statements,[45] these have so far looked more at the implications on sovereignty when it comes to operations impacting on the territory of the State affected, and, with the notable exception mentioned above, not so much when it comes to the relationship between an international organization and its host State. In this area, different States may have different and diverging views as to how they interpret those concepts, and some may not have a clear, public position as to their interpretation of this area of law. It is therefore important to ensure that questions which may affect an organization's capacity to operate are addressed by it in its dialogue with its host State.

In other words, would a cyber host State consider an operation targeting an organization hosted on its territory as a violation of its sovereignty? If so, under what conditions? Could the cyber host State in that case seek countermeasures against the perpetrators? If so, which countermeasures? If the operation is being run through infrastructure on the territory of a third State, would the cyber host State seek to get the cooperation of the third State in order to bring the operation to an end? Would the cyber host State refer to a due diligence obligation of the third State to bring the operation to an end? Would any of the above constitute a concern for the organization, insofar as the intervention of the cyber host State may affect and compromise its neutrality, impartiality and independence?

43 See "Scenario 04: A State's Failure to Assist an International Organization", in Kubo Mačák, Tomáš Minárik and Taťána Jančárková (eds), *Cyber Law Toolkit*, available at: https://tinyurl.com/3m4nm6nv.

44 See, for example, Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017, available at: https://ccdcoe.org/research/tallinn-manual/.

45 See French Ministry of Defence, *International Law Applied to Operations in Cyberspace*, 2019, available at: www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

Dialogue with the State/government where the organization wants to deploy/offer digital services

For an organization like the ICRC, working in areas of armed conflict and other situations of violence, dialogue with the State in which it would operate is an essential step to ensuring acceptance of the deployment of digital humanitarian services.

This is not an anodyne statement, particularly taking into account that, as set out above, such services must be exclusively humanitarian services, and offered in a neutral, impartial and independent way. This means that affected people expect that any communication with or data provided to the humanitarian organization will not be accessed and used by third parties for non-humanitarian purposes. Similarly, the State in question must accept this protected digital humanitarian space and not interfere with it or with the technical measures used by the humanitarian organization to protect it.[46]

Similarly, this dialogue should also aim at ensuring that "humanitarian data flows" directed to the organization are not affected by internet shutdowns, and that affected populations have access, to the maximum extent possible, to connectivity.

Dialogue with State and State-sponsored attackers

Securing the organization's cyber perimeter against the technical capabilities of State-led or State-sponsored attackers, and in some cases also of certain groups linked to non-State armed groups, is a major challenge. A humanitarian organization will most likely never have sufficient resources to counter the offensive power of these types of adversaries. From the point of view of an organization like the ICRC, which bases its security on acceptance and respect of its humanitarian mandate, the primary objective would be to ensure acceptance of a protected digital humanitarian space.

Just like the organization routinely does in the non-digital world, this requires it to consider how to securely carry out a bilateral confidential dialogue with States, State-sponsored groups and groups linked to non-State armed groups with sophisticated capabilities, potentially including hacker groups, in order to explain its work, mandate and *modus operandi*, to establish respect for its digital humanitarian space, to prevent adverse cyber operations and, thereby, to negotiate and obtain "digital access". In this respect, key questions will arise as to how, technically, the organization can in practice set up a bilateral confidential

46 See Group of Friends of the Protection of Civilians in Armed Conflict, statement submitted to the UN Security Council Arria-Formula Meeting on Cyber-Attacks against Critical Infrastructure, New York, 26 August 2020, available at: www.eda.admin.ch/dam/mission-new-york/en/speeches-to-the-un/2020/20200826-new-york-POC-GoF%20PoC%20statement_E.pdf. "The trust of the people they serve is the currency of humanitarian organizations. This trust is a precondition for humanitarian action. Therefore, we, as Members [*sic*] States, must create an environment, including a safe information infrastructure that allows humanitarian organizations to successfully carry out their mandate. The Resolution on Restoring Family Links adopted at the 33rd International Conference of the Red Cross and Red Crescent in 2019 constitutes an important step in this direction."

dialogue with these actors, and in particular with State-sponsored hacker groups (and be sure it is with them that it is indeed having the dialogue). In order to maintain the trust of all stakeholders in the international community, it is also important that the organization is transparent about the existence, reasons and objectives of this dialogue. As explained on the ICRC web pages that clarify who the ICRC engages in dialogue with, and why:

> It is those who carry weapons who can kill – and be killed. It is also they who can facilitate or hinder humanitarian action. The ICRC therefore maintains a dialogue with all weapon bearers, State and non-State, as part of our mandate to protect and assist people affected by war and other violence.[47]

This is true both in the physical world and in cyberspace.

This confidential dialogue should be complemented with state-of-the-art security[48] and, where possible, research and development partnerships with academia to go one step further than state-of-the-art security. Although it is most likely very difficult to ensure security at a level sufficient to counter a State-sponsored actor in all circumstances, the level of security to be put in place should be guided by (1) due diligence – i.e., applying a level of security that can be expected from an organization handling highly sensitive data, taking into account the cost of technology, sensitivity of the information, and state of the art; and (2) the aim of raising the cost (in terms of financial resources, time, and staff required to carry out adverse cyber operations, as well as reputational repercussions) of adverse operations that successfully affect the organization, to a level that such operations are not worth the cost of achieving them. It is suggested that a combination of these two elements is necessary to ensure effective protection.

Conclusion

An international humanitarian organization going through a process of digital transformation and aiming to offer digital services directly to beneficiaries faces numerous questions that are extremely novel. These questions range from the legal and organizational to the technical and operational, and relate to issues that are transversal and highly interdependent – and at present none of them have any clear and unequivocal answers.

It is fundamental, therefore, that any organization which becomes an actor in cyberspace carries out an in-depth analysis of the questions discussed in the present paper and identifies the answers that are suitable for the organization based on its status, mandate and working modalities. Furthermore, these answers

47 See ICRC, "Dialogue with Weapon Bearers", available at: www.icrc.org/en/what-we-do/building-respect-ihl/dialogue-weapon-bearers.

48 See ENISA, "What Is 'State of the Art' in IT Security?", 7 February 2019, available at: www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.

need to be formulated in a clear cyber security strategy informing the organization's stance in cyberspace, as well as its decisions to prioritize investment areas and its allocation of resources.

In addition to a cyber strategy developed on these bases, international humanitarian organizations need to consider unique and specific technical solutions to their specificities, such as the creation of a "digital humanitarian space" along the model of a "sovereign cloud" or a "digital embassy". These do not currently exist as part of any commercial offering, primarily because technological commercial offerings are developed based on the demands of the majority of customers, who, unlike international humanitarian organizations, are not entitled to rely on privileges and immunities from the jurisdictional control of at least one State.

Partnerships with academia and industry are an important part of this effort, but they alone are not sufficient – what is essential is both (1) wider political will on the part of external stakeholders to guarantee the protection of a digital humanitarian space, and (2) the awareness, knowledge, focus and determination of internal stakeholders to genuinely preserve the independence, impartiality and neutrality of international humanitarian organizations in cyberspace. Without this, international humanitarian organizations will inevitably be pushed into accepting solutions that are unsuitable for the work they are mandated to carry out.