International Review of the Red Cross (2022), **104** (919), 1267–1284.
Selected Articles
doi:10.1017/S1816383122000194

IRRC_

The SolarWinds hack: Lessons for international humanitarian organizations

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

Abstract

As humanitarian organizations become more active in the digital domain and reliant upon new technologies, they evolve from simple bystanders to full-fledged stakeholders in cyberspace, able to build on the advantages of new technologies but also vulnerable to adverse cyber operations that can impact their capacity to protect and assist people affected by armed conflict or other situations of violence. The recent hack of the International Red Cross and Red Crescent Movement's Restoring Family Links network tools, potentially exposing the personal data of half a million vulnerable individuals to unauthorized access by unknown hackers, is a stark reminder that this is not just a theoretical risk but a very real one.[1]

The 2020 cyber operation affecting SolarWinds, a major US information technology company, demonstrated the chaos that a hack can cause by targeting digital supply chain components. What does the hack mean for the humanitarian cyberspace, and what can we learn from it? In this article, Massimo Marelli, Head of the

* 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 Ben Hayes, Fabien Caparros, Bruno Demeyere, Kubo Mačák, Pierrick Devidal, Martin Schuepp, Hugo Van Den Eertwegh, Justinas Sukaitis and Cedric Maire for their valuable feedback on an earlier draft. Special thanks go to Vincent Graf Narbel, Mathias Blarer and Zilin Wang for their input and research support, particularly on the technical aspects addressed in this article. All errors are the author's own.

International Committee of the Red Cross's Data Protection Office, draws out some possible lessons and considers the way forward by drawing on the notion of "digital sovereignty".

Keywords: supply chain, cyber security, digital sovereignty, data sovereignty, humanitarian action, international law, data protection, cyber strategy, international organizations.

Introduction

Even in 2022, with a news cycle overwhelmed by conflicts, a deadly pandemic, climate disasters and political turmoil, the 2020 cyber operation targeting SolarWinds continues to leave a mark, with consequences that still persist today.[2] Hackers used the operation against SolarWinds, a major US information technology (IT) company, to spy on private companies – such as FireEye,[3] the elite cyber security firm that exposed the breach[4] – as well as US government agencies, including the Department of Homeland Security and Treasury Department.

Cyber operations of this type, exploiting the digital supply chain, are happening and causing damage. Humanitarian organizations today are essentially bound to this supply chain and therefore are also in harm's way.[5] This article will explore these two phenomena and discuss avenues forward. Specifically, the article seeks to identify relevant questions and draw lessons from the SolarWinds hack in order to help illustrate the challenges facing humanitarian organizations in cyberspace and, in turn, to think through the potential approaches that organizations can take to meet these challenges.

There are three parts to this article. The first part provides a brief analysis of the SolarWinds hack and its significance to international organizations and

[1] International Committee of the Red Cross (ICRC), "Cyber-Attack on ICRC: What We Know", 16 February 2022, available at: www.icrc.org/en/document/cyber-attack-icrc-what-we-know (all internet references were accessed in March 2022).

[2] A simple explanation of how the hack happened and why it is so significant can be found in Isabella Jibilian and Katie Canales, "The US is Readying Sanctions against Russia Over the SolarWinds Cyber Attack", *Insider*, 15 April 2021, available at: www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[3] William Turton and Kartikay Mehrota, "FireEye Discovered SolarWinds Breach while Probing Own Hack", *Bloomberg*, 15 December 2020, available at: www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack.

[4] See FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chains to Compromise Multiple Global Victims with SUNBURST Backdoor", *Mandiant*, 13 December 2020, available at: www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

[5] Though not directly the subject of this paper, humanitarian organizations face very significant and real cyber risks, as seen in the February 2022 hack of the International Red Cross and Red Crescent Movement's Restoring Family Links network tools, which potentially exposed the personal data of half a million vulnerable individuals to unauthorized access by unknown hackers. For more, see ICRC, above note 1.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

humanitarian action. The second part places the SolarWinds hack and the challenges it poses in a broader context, drawing on the concepts of "data sovereignty" and "digital sovereignty"; the application of humanitarian principles and working modalities in conflict scenarios; and the broader geopolitical drivers of overarching conflicts in cyberspace. The third part of the article considers how international humanitarian organizations like the International Committee of the Red Cross (ICRC) can respond, taking all of these factors into account.

SolarWinds: The hack and its significance

While the Stuxnet operation[6] showed us that, when attackers have sufficient means, it is very challenging to resist thoroughly planned and targeted operations (including, in that case, targeting air-gapped systems), the SolarWinds hack has shown us the massive scale and reach that an adversary can achieve by targeting digital supply chain components that are widely adopted, in this case the security of the software supply chain.

The SolarWinds hack[7] was an operation that was ongoing during most of 2020. It was revealed and widely reported in the media at the end of December 2020. It primarily targeted US government agencies and private companies, including the security company that exposed the hack, FireEye. The European Commission confirmed on 13 April 2021 that fourteen institutions, bodies or agencies of the European Union used SolarWinds/Orion. Six of them were confirmed to have been affected by the hack.[8] The operation is believed by the US intelligence community to be of Russian origin[9] and has been formally attributed by the United States to the Russian Federation.[10] Russia has denied any involvement in the operation.[11] The SolarWinds hack was a "supply chain" type of operation in that it vectored malware through updates of the Orion software product of SolarWinds, which is widely used to manage IT resources along business supply chains. The malicious code creates a backdoor to customers' systems, which enables hackers to install more malware and to spy on their victims. Even at the

[6] Stuxnet is a well-known operation carried out in Iran, allegedly by the United States and Israel, and first reported in June 2010. It involved damaging a number of centrifuges installed in the Natanz nuclear facilities used for fuel enrichment. It was allegedly aimed at hindering the Iranian uranium enrichment programme. For more information, see "Stuxnet (2010)", *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/w/index.php?title=Stuxnet_%282010%29.

[7] I. Jibilian and K. Canales, above note 2.

[8] European Parliament, "Answer Given by Mr. Hahn on Behalf of the European Commission", 13 April 2021, available at: www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.pdf.

[9] Government of the United States, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)", 5 January 2021, available at: www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[10] White House, "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government", 15 April 2021, available at: www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[11] "'Flattered' Russian Spy Chief Denies SolarWinds Attack", *Reuters*, 18 May 2017, available at: www.reuters.com/technology/russian-spy-chief-denies-svr-was-behind-solarwinds-cyber-attack-bbc-2021-05-18/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

time of writing, months after the hack was revealed, the full extent of the damage cannot yet be completely mapped. Indeed, according to the CEO of FireEye, Kevin Mandia, the hackers prioritized stealth above all else.[12] It has been estimated that recovering from the SolarWinds hack could take up to eighteen months.[13]

It has also been reported that "[w]hile the SolarWinds hack primarily targeted in-house infrastructure, the breach has morphed into a multidimensional assault on key computing infrastructure, including cloud services".[14] Indeed, it appears that breaching large-scale cloud providers, such as Microsoft,[15] was a primary objective of the operation,[16] and this in turn exposed the customers of such providers to data breaches. Microsoft's president, Brad Smith, has suggested that more than 80% of the victims subsequently targeted were non-government organizations.[17] Microsoft source code was also accessed,[18] and it appears that SolarWinds hackers also accessed the US Justice Department's Microsoft Office 365 email environment.[19]

Supply chain attacks and their challenges

A supply chain attack occurs when hackers infiltrate a victim's IT systems through an outside partner or vendor that provides components of the system, ranging from silicon chips to software applications.[20] In recent years the attack surface of IT systems has drastically increased due to their increased complexity and that of their supply chains.[21] Broadly speaking, there are two types of supply chain

[12] Lucian Costantin, "SolarWinds Attack Explained: And Why It Was so Hard to Detect", *CSO*, 15 December 2020, available at: www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

[13] Patrick Howell O'Neill, "Recovering from the SolarWinds Hack Could Take 18 Months", *MIT Technology Review*, 2 March 2021, available at: www.technologyreview.com/2021/03/02/1020166/solarwinds-brandon-wales-hack-recovery-18-months/.

[14] Alicia Hope, "Cloud Services from Major Providers Including Amazon and Microsoft Vulnerable to the Widespread SolarWinds Hack", *CPO Magazine*, 4 January 2021, available at: www.cpomagazine.com/general/cloud-services-from-major-providers-including-amazon-and-microsoft-vulnerable-to-the-widespread-solarwinds-hack.

[15] Scott Ikeda, "Hackers Behind SolarWinds Supply Chain Attack Targeted CrowdStrike through Microsoft Vendor's Account", *CPO Magazine*, 31 December 2020, available at: www.cpomagazine.com/general/hackers-behind-solarwinds-supply-chain-attack-targeted-crowdstrike-through-microsoft-vendors-account.

[16] *Ibid.*

[17] Katie Canales, "The US Senate Just Grilled Microsoft and SolarWinds Over Last Year's Historic Cyberattack. Here's What Happened", *Insider*, 23 February 2021, available at: www.businessinsider.com/watch-live-senate-hearing-solarwinds-microsoft-fireeye-crowdstrike-cyberattack-2021-2.

[18] Ravie Lakshmanan, "Microsoft Says SolarWinds Hackers Accessed Some of Its Source Code", *The Hacker News*, 31 December 2020, available at: https://thehackernews.com/2020/12/microsoft-says-solarwinds-hackers.html.

[19] *Ibid.*

[20] Maria Korolov, "Supply Chain Attacks Show Why You Should Be Wary of Third-Party Providers", *CSO*, 4 February 2021, available at: www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.

[21] Krontech, "The Increasing Attack Surface in 2019", 15 April 2019, available at: https://krontech.com/the-increasing-attack-surface-in-2019.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

attack, software and hardware, though the underlying technological infrastructure is much more complex in practice.[22] The SolarWinds hack is a perfect example of supply chain attacks where the hackers attack the software applications of the systems. Other examples of this kind of operation, which has been prevalent for many years, include dependency confusion attacks,[23] a type of software supply chain attack that relies on the dependencies inherent in software development processes, discovered by bug hunter Alex Birsan. For many package managers (such as npm and pip), the catalogue of dependencies for software can be a mix of public and private dependencies, which causes ambiguity when there exist both public and private packages with the same name. Some package managers default to public packages over private ones upon a name conflict. By exploiting this, the hackers can upload their malicious package to the package manager registry with the same name as some private packages used by the victim's software. The victim will run the malicious code directly on its local environment upon software build. As explained in Birsan's blog, this vulnerability enabled him to hack into systems belonging to Apple, Microsoft and other major tech companies without much effort.[24]

Examples of hardware supply chain hacks include the Supermicro hack.[25] According to a Bloomberg report, Chinese hackers planted, during the manufacturing phase, small compromised chips on Supermicro motherboards[26] that were destined to be used in US government data centres as well as in the data centres of large cloud technology companies. The chips in question contained a backdoor programmed to send data back to the hackers. While, according to the Bloomberg report, both Supermicro and China separately deny the allegations, the elements reported by Bloomberg describe a useful illustration of a scenario of a possible hack on the hardware level of the supply chain. Another known example of a supply chain attack relates to Crypto AG, a Swiss company supplying States with hardware devices for encrypting confidential communications. As revealed in a Swiss parliamentary investigation in 2020, Crypto AG machines included secret backdoors to US intelligence services which provided Crypto AG with full access to the content of the communications.[27]

[22] "Layers of Computing Systems", *David 'n' CS*, 1 September 2016, available at: https://davidncs.wordpress.com/2016/09/01/featured-content-2/.

[23] Alex Birsan, "Dependency Confusion: How I Hacked into Apple, Microsoft and Dozens of Other Companies", *Medium*, 9 February 2021, available at: https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610.

[24] *Ibid.*

[25] Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a US Tech Supplier", *Bloomberg*, 12 February 2021, available at: www.bloomberg.com/features/2021-supermicro/.

[26] Linsey Knerl, "What Does a Motherboard Do?", HP, 17 October 2019, available at: www.hp.com/us-en/shop/tech-takes/what-does-a-motherboard-do.

[27] Greg Miller, "The Intelligence Coup of the Century", *Washington Post*, 11 February 2020, available at: www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

As US public-interest technologist Bruce Schneier, speaking from a US perspective, explains:

> Supply-chain security is an incredibly complex problem. US-only design and manufacturing isn't an option; the tech world is far too internationally interdependent for that. We can't trust anyone, yet we have no choice but to trust everyone. Our phones, computers, software and cloud systems are touched by citizens of dozens of different countries, any one of whom could subvert them at the demand of their government.[28]

Humanitarian security in cyberspace

Humanitarian organizations have growing digital footprints and are increasingly dependent on the international supply chains that the SolarWinds hack has exposed as vulnerable. As described by this author in a previous contribution for the *Review*,[29] there are several key operational, technical, organizational and legal elements that an international humanitarian organization should consider when increasing its footprint in the cyber sphere, and it is important for humanitarian organizations to clearly address these elements in a cyber security strategy. The key starting point in the development of a cyber security strategy for a humanitarian organization is an analysis of the cyber environment within which the organization operates and the challenges and threats it faces therein. In addition, in developing a cyber security strategy, humanitarian organizations should take into account that the principles of humanity, neutrality, impartiality and independence, as well as humanitarian working modalities developed over the years to enable humanitarian work, require strategic transposal in order to reflect such organizations' presence and activities in cyber space, deriving, for example, from the offering of humanitarian services to affected communities digitally.[30]

In addition to these elements, and as will be seen further in this article, it is argued that, in developing a cyber security strategy, it is important for humanitarian organizations to take into account three specific dimensions of the cyber environment in which they operate. The first of these is the challenges that international organizations face in maintaining exclusive "jurisdictional control" over their data due to the complexity and interconnectedness prevalent in cyberspace. The second is the challenges of applying the humanitarian principles through which organizations like the ICRC have garnered trust and access in the real world to cyberspace. What lessons can be drawn from the attempts to mitigate security risks in environments characterized by conflict and other

[28] Bruce Schneier, "Supply-Chain Security", *Security Boulevard*, 10 May 2018, available at: https://securityboulevard.com/2018/05/supply-chain-security/.

[29] Massimo Marelli, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red Cross*, Vol. 102, No. 913, 2020.

[30] *Ibid.*

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

situations of violence – threats which may come from State and non-State actors alike? The third dimension is the broader geopolitical cyber environment in which international humanitarian organizations operate. Parallels emerge with the power struggles that often underlie the conflicts to which humanitarians respond, and the very real risk of being caught in the crossfire.

"Data sovereignty" and "digital sovereignty": Tools for protecting humanitarian principles in cyberspace

The privileges and immunities enjoyed by international humanitarian organizations are an essential means of ensuring the neutrality and independence of their humanitarian action, which is the basis for trust on the part of the communities they serve. Anything that calls into question the neutrality and independence of organizations like the ICRC threatens to undermine that trust, which in turn jeopardizes the viability of operations on the ground and access to those in need of assistance. The security and confidentiality of information given to the ICRC in confidence, for example by detainees or parties or witnesses to a conflict, is fundamental to maintaining the trust that the organization has built up over 150 years. Accordingly, how can the ICRC maintain that trust when operating in digital environments, with incidents like the SolarWinds hack demonstrating how vulnerable the IT systems that international entities use can be?

These challenges are not unique to the ICRC, of course. States, public bodies and multinational enterprises face similar challenges. Some States have responded by asserting the need for "data sovereignty" or "digital sovereignty".[31] Both of these concepts imply a problematic technological dependency embedded in unwarranted or undesirable international relations, yet for the most part they are rarely defined or unpacked. And despite implying distinct types of sovereignty, these terms are often used interchangeably, without reference to how one concept might be distinguished from the other. It is therefore instructive to try to disentangle these terms.

While the notions of data sovereignty and digital sovereignty have a very different meaning from the notion of sovereignty under international law, they borrow loosely from the international law notion of the territorial sovereignty of a State: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[32] This brings a connotation of control over the use of data and digital infrastructure. Data sovereignty would appear to indicate that a State (or an international

[31] See, for example, Marie Baezner and Patrice Robin, "Cyber Sovereignty and Data Sovereignty", ETH Zürich Research Collection, 2018, available at: https://doi.org/10.3929/ethz-b-000314613; Stéphane Couture, "The Diverse Meanings of Digital Sovereignty", *Global Media Technologies & Cultures Lab*, 5 August 2020, available at: https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/; Patrik Hummel, Matthias Braun, Max Tretter and Peter Dabrock, "Data Sovereignty: A Review", *Big Data & Society*, Vol. 8, No. 1, 2021.

[32] Permanent Court of Arbitration, *Island of Palmas Case (or Mianga), United States v Netherlands, Award*, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4 April 1928.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

organization) can exercise full control over the data it processes (which are not in the public domain), to the exclusion of any (other) entity. In other words, no other State may by application of law seek and obtain the data of the "data sovereign". For the avoidance of doubt, the notion of sovereignty is used analogously, since international organizations obviously do not enjoy territorial sovereignty. Rather, an international organization may seek to leverage the privileges and immunities it enjoys, including the inviolability of its correspondence and archives and its immunity from jurisdiction, in combination with other organizational and technical measures to achieve "exclusive control" over data. As suggested elsewhere,[33] international organizations can seek to ensure exclusive control through a combination of legal, technical and organizational measures.[34]

While the notion of data sovereignty helps to crystalize the challenges faced by States and international organizations in transnational environments like the contemporary Internet, it is not comprehensive enough to capture the challenges posed by supply chain attacks like SolarWinds. Put another way: even if by a combination of legal, technical and organizational measures an organization manages to establish exclusive control over the data it processes, largely addressing concerns over possible loss of control through exercise of legal process, a lack of control over its supply chain leaves it exposed to additional risks and vulnerabilities. Data sovereignty, it appears, needs to be complemented by a more nuanced strategic approach, which could be encapsulated by the notion of digital sovereignty.

Like data sovereignty, digital sovereignty[35] is difficult to define. It appears to imply a broader form of "sovereign" control that covers not just data but also the hardware and software supply chains, as mentioned above, as well as network infrastructure (cables, routers and switches) and the communications supply chain. The concept of digital sovereignty does not necessarily mean that a State or an international organization can produce or have total control over all of the above, in a "digital autarky" sense: considering the level of dependencies and interconnectedness of cyberspace today, this may well be beyond the reach of even the most powerful and sophisticated stakeholders in cyberspace who have strategically been investing huge resources precisely for this purpose.[36] Indeed, the enormity of these challenges may even call into question the appropriateness of using the term "digital sovereignty" in the first place, when the most that can realistically be achieved may be "digital independence". But just as data sovereignty is helpful in understanding challenges, vulnerabilities and

[33] M. Marelli, above note 29.

[34] Linked to this is the notion of the "sovereign cloud" – i.e., a cloud architecture in which data sovereignty can be respected and applied. See Christopher Kuner and Massimo Marelli, *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC, Geneva, 2020, Chap. 10.9, available at: www.icrc.org/en/data-protection-humanitarian-action-handbook.

[35] European Commission, "Europe: The Keys to Sovereignty", 11 September 2020, available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.

[36] See, for example, Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security*, Vol. 44, No. 1, 2019.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

international relations, digital sovereignty as a term points to the underlying fundamental objective of asserting control and exercising discretion in the choice and use of digital tools and infrastructures, pointing in other words to the importance of managing and mitigating "digital dependencies", and over-dependencies in particular.

While ensuring data sovereignty would already be a major success for any international humanitarian organization, because it would enable a response to most of the digital challenges identified so far, the recent SolarWinds hack highlights that this analysis should perhaps be taken one step further. International humanitarian organizations ought to give attention to their digital sovereignty too.

It is argued that carefully analyzing the application of the notion of digital sovereignty to the work of humanitarian organizations may provide these organizations with security assets that are linked to, and exist because of, their unique status, and that can be relied on in addition to and beyond what technical security measures alone can offer. In the humanitarian sector, the reaction to cyber attacks such as the SolarWinds hack is often defeatist: if the most renowned government agencies and security companies cannot protect themselves from cyber attacks and surveillance, is it even worth it for a humanitarian organization to try to protect itself? Another common reaction is to lean even more on cyber security "professionals", tech giants and "hyperscalers" equipped with very significant resources and skilled workforces. Both reactions, however, fail to take into account the fact that security is not an absolute concept and that it depends on the vulnerabilities, threats, assets and opportunities of each organization.

The SolarWinds hack has shown us that even the best-resourced, tech-giant-backed security teams, such as those of some of the companies that relied on SolarWinds, can fail in protecting their customers, and that, precisely because they serve so many customers, it does not matter who the target is: every organization using affected cloud services becomes vulnerable, and a potential victim of the attack – and that includes humanitarian organizations. Yet, some humanitarian organizations have specific "security enablers" that other organizations do not have. For instance, the security enablers of the ICRC include the recognition of a specific mandate under international law to pursue its exclusively humanitarian mission, and the trust and acceptance generated by its principles of neutrality, impartiality and independence, as well as operating modalities based on (among others) confidentiality and bilateral confidential dialogue. The ICRC is used to leveraging these principles and operating modalities for its own security in the physical world, and like other international humanitarian organizations, it needs to transpose this way of working to the cyber world.[37]

[37] Massimo Marelli, "Hacking Humanitarians: Moving Towards a Humanitarian Cybersecurity Strategy", *Humanitarian Law and Policy Blog*, 16 January 2020, available at: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

Ensuring the security of humanitarian actors in cyberspace

For over 150 years, the ICRC has been operating in conflict areas that are increasingly fragmented, polarized, volatile and difficult to read, where technical innovation has often brought important challenges. The ICRC has therefore been keenly aware of the vulnerable situation it is in. Specific security rules consider that in some places, walking down the street or in a market could be too dangerous; staff could get abducted or sometimes even killed simply because they are foreigners and/or they work for a humanitarian organization. In those cases, security rules provide for movement restrictions, and staff are not allowed to leave the compound of the organization unless specific security measures are in place. It is also possible that vehicles of the organization, moving in order to deploy and run its activities, may hit an improvised explosive device or be attacked, possibly by accident. Therefore, security rules provide for restrictions of movement along specifically greenlighted routes, notifying all the parties to the conflict or actors involved in a situation of violence about the anticipated movement in the area, and marking the organization's vehicles very visibly with emblems and flags in order for them to be recognized from afar.

This approach also relies on the assumption that a very important protective asset that humanitarians working amid conflict and violence can have and rely on is the trust and acceptance of warring parties, local authorities and populations.

The notion that the security of humanitarian staff is linked to trust and perceptions of neutrality, impartiality and independence is indeed one of the pillars of security for organizations like the ICRC. Acceptance is a key pillar of security that highlights the need to be politically, operationally and culturally accepted as a neutral, impartial and humanitarian actor by all relevant stakeholders – it is an essential operational modality that contributes to access and security. Specific security rules are therefore in place to ensure that humanitarian workers demonstrate at all times the humanity, neutrality, impartiality and independence that may grant them the trust and acceptance (or at least tolerance) of all relevant stakeholders.

This principled approach is further reinforced by a risk management-based security system that provides practical guidance for field staff as it navigates the acceptance–rejection sliding scale on a daily basis. This includes making sure that humanitarian personnel do not become "collateral damage" to an attack. For example, the ICRC would generally not locate an office within, or in proximity to, a military base. Nor would, in principle, an ICRC office or ICRC staff be protected by military personnel of one of the two parties to a conflict or actors in a situation of violence, as this would negatively affect its perception as a neutral and impartial humanitarian actor. It is for instance a common practice that humanitarian vehicles in transit must drive at a safe distance from military convoys.

While a parallel between the physical world and cyberspace is not straightforward and may be imperfect, there are reasons to consider that a similar

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

approach – even if more technically challenging – could be transposed to cyberspace. By depending too much on the technology solutions, systems and networks that are increasingly recognized as compromising digital sovereignty, a humanitarian organization runs the risk of going against the logic of the security rules and principles mentioned above.

While it may be stretching things to suggest that the use of or dependence on these tools calls into question a humanitarian organization's neutrality, impartiality and independence, and in turn has an impact on its acceptance (or tolerance) and its security, it is simply a fact that the use of and dependence on these tools makes a humanitarian organization vulnerable to attacks aimed at the great powers that rely on them – just as a humanitarian organization could be the victim of a rocket attack on a military base if it had its office physically located within the base.

It may be that the "classic" humanitarian approach to security as set out above is not fully suitable for the digital sphere. But the above analysis does highlight that alternative approaches need to be looked for and considered, whether these may lead to already available tools and solutions or, more likely, to new tools that need to be designed and built.

Humanitarians in the crossfire?

The SolarWinds attack is merely the latest manifestation of what is currently unfolding in cyberspace: a competition between the "great powers". David Kilcullen and others have analyzed this power struggle, including in cyberspace, stressing that what is at stake is not a series of isolated, one-off cyber incidents of a criminal nature, but a worldwide and increasingly strategic use of cyberspace to assert influence, and dominance, by global powers.[38]

Any international humanitarian organization that operates in a complex and volatile conflict environment on the basis of neutrality, impartiality and independence must remain alert to these geopolitical dynamics, since they have an impact on the physical world in which such organizations function. As a result, these organizations need to ground their planning in a robust strategy that captures the implications of the great powers' competition, and in this respect, what works for a multinational corporation may not necessarily work for an international humanitarian organization.[39]

Against the backdrop of these global tensions among the major cyber powers, one could ask whether using the same digital supply chain as one of the key stakeholders, and counting on the security it provides, brings a humanitarian organization dangerously close to the physical-world parallel of positioning offices within or near a military base. While the infrastructure of the base may

[38] David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West*, Oxford University Press, New York, 2022.

[39] M. Marelli, above note 37.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

look reassuring, relying on it may affect the perception that other stakeholders have of the organization's neutrality, impartiality and independence. It cannot be excluded that this, in turn, may affect the trust and acceptance that enables the organization to deliver on its exclusively humanitarian mandate. Even if the perception of the organization's neutrality, impartiality and independence is not affected, it could find itself caught in the crossfire if the military base is attacked, simply because of its proximity to the target.

While examining the threats from this angle takes into account just one of the many risks that hackers may pose, it does provide an important additional security enabler to leverage for protection from possible cyber operations by States and State-sponsored groups, or by non-State armed groups participating in the great powers' competition dynamics. Arguably these are the more powerful, and well-resourced, types of attackers.

Tackling the challenge: Forward-looking proposals

Given the challenges laid out above, one question is pivotal: are there any alternatives to relying on the same supply chain as that which is used by possible targets?

The answer, unfortunately, is: not yet. There is no viable alternative for the entire stack of technology supporting the humanitarian cyber infrastructure, from hardware, to software, to networks, and beyond. The digital infrastructures we are using today have become increasingly complex. Digital systems are made of hardware and software that can be infiltrated in various ways, in particular on the supply chain. Indeed, according to former CIA and NSA director Michael Hayden, supply chain threats are not "a problem that can be solved" but "a condition that you have to manage".[40]

In this sense, digital sovereignty can be seen as a risk management problem with respect to digital supply chain threats. The asset at risk is an organization's digital infrastructure, including both software and hardware, but eventually also the organization's ability to carry out its mandate and mission. A successful strategy around digital sovereignty is therefore one that consists of the continuous assessment and management of risks related to the digital supply chain.

Risk mitigation tools from within the supply chain

There are several avenues being explored and worked on that can be useful as risk mitigation tools in this area. These avenues make sense for all organizations and are not of exclusive relevance for impartial humanitarian organizations, but they are ones that an organization of this type, having identified the supply chain as a particularly delicate area, may wish to consider as a priority.

[40] Adam Rawnsley, "Can Darpa Fix the Cybersecurity 'Problem from Hell'?", *Wired*, 8 May 2011, available at: www.wired.com/2011/08/problem-from-hell/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

The first one is based on the notion that, even if each digital component on its own cannot be fully trusted, it is possible to build trustworthy and resilient systems out of untrustworthy components. As security researcher Bruce Schneier has explained:

> The other solution is to build a secure system, even though any of its parts can be subverted. … [C]an we solve [supply chain issues] by building trustworthy systems out of untrustworthy parts? It sounds ridiculous on its face, but the Internet itself was a solution to a similar problem: a reliable network built out of unreliable parts. This was the result of decades of research. That research continues today, and it's how we can have highly resilient distributed systems like Google's network even though none of the individual components are particularly good. It's also the philosophy behind much of the cybersecurity industry today: systems watching one another, looking for vulnerabilities and signs of attack.[41]

In other words, minimize trust to maximize trustworthiness.[42] "Zero trust" is an approach that goes in this direction. The National Institute of Standards and Technology (NIST) refers to the notion of "zero trust" as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised".[43] The main principles and technologies behind zero-trust security involve an assumption that an attacker could be both within and outside of the network, and that users within a network should not be assumed to be trusted. They include least-privilege access, microsegmentation, multi-factor authentication, and strict controls on device access.[44]

Many new technologies like distributed ledgers,[45] homomorphic encryption[46] and confidential computing[47] are designed to work under this assumption of a hostile environment. While their application would be very useful in enabling trust in an untrusted environment, some of these technologies are not yet mature enough to be fully deployed, and they are still being explored in research and development mode. It is therefore important to invest in partnerships to further leverage these advances in technology, such as the

[41] Bruce Schneier, "Every Part of the Supply Chain Can Be Attacked", *New York Times*, 25 September 2019, available at: www.schneier.com/essays/archives/2019/09/every_part_of_the_su.html.

[42] David Basin, Patrick Schaller and Michael Schläpfer, *Applied Information Security: A Hands-On Approach*, Springer, Berlin, 2011.

[43] Scott W. Rose, Oliver Borchert, Stu Mitchell and Sean Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, August 2020, p. 4, available at: ww.nist.gov/publications/zero-trust-architecture.

[44] Cloudflare, "Zero Trust Security: What Is a Zero Trust Network?", available at: www.cloudflare.com/learning/security/glossary/what-is-zero-trust/.

[45] "Distributed Ledger", *Wikipedia*, available at: https://en.wikipedia.org/wiki/Distributed_ledger.

[46] Microsoft, "Homomorphic Encryption", 27 March 2016, available at: www.microsoft.com/en-us/research/project/homomorphic-encryption/.

[47] Azure, "Azure Confidential Computing", available at: https://azure.microsoft.com/en-us/solutions/confidential-compute/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

partnerships that the ICRC recently launched with the Swiss Federal Institutes of Technology in Lausanne[48] and Zurich.[49]

In addition, establishing security standards for hardware and software can contribute to mitigating risks linked to supply chains. In its early days, aviation was also a sector that involved high risks; little or no governance was in place to guarantee the safety of aircraft, and passengers flew at their own risk.[50] Today, the aviation industry is subject to extensive quality norms and testing requirements, and aircraft manufacturers are held accountable for defects found in the aircraft. Similarly, investing in the creation of minimum security standards for hardware and software, and holding suppliers accountable for violations of these standards, could go a long way in mitigating supply chain security risks.

Another key avenue in the mitigation of digital supply chain risks is the removal of strong supplier dependencies. In terms of digital sovereignty, vendor lock-in without the possibility of moving from one vendor to another – for example, because of product incompatibilities, lack of interoperability or portability, or because there may be no alternative in the market – is a major concern. Such dependencies bear various risks: if the vendor goes out of business, it can no longer provide support for its products or patches to address discovered vulnerabilities. Also, the vendor can suddenly change its policies and pricing to the detriment of the customer, or even stop delivering its products and services as a form of digital sanction.

To address the risks linked with vendor dependencies of this type, free and open-source alternatives can be considered. An interesting initiative in this respect was the MALT Project at the European Organization for Nuclear Research (CERN),[51] which was aimed at implementing a strategy to seek "open software solutions and products with simple exit strategies and low switching costs". Free and open-source software (FOSS)[52] can be seen as a method for mitigating dependencies; it is usually developed through the collaboration of an open community, and can be publicly reviewed and modified, and used for any purpose.[53] However, it should be noted that FOSS comes with its own supply chain risks, and under the cover of improvements, malicious contributors can

[48] EPFL, "EPFL, ETH Zurich and the ICRC Team Up to Bolster Humanitarian Aid", 10 December 2020, available at: https://actu.epfl.ch/news/epfl-eth-zurich-and-the-icrc-team-up-to-bolster-hu/.

[49] ETH Zürich, "Engineering at the Service of Humanitarian Aid", 10 December 2020, available at: https://ethz.ch/en/news-and-events/eth-news/news/2020/12/cooperation-icrc.html.

[50] Digital Switzerland, *Supply Chain Security*, 26 September 2019, p. 14, available at: https://digitalswitzerland.com/wp-content/uploads/2021/08/White_Paper_Supply_Chain_Security_2019_09_25_EN.pdf.

[51] Andrew Purcell, "Three-Year MALT Project Comes to a Close", CERN, 17 January 2022, available at: https://home.cern/news/news/computing/three-year-malt-project-comes-close.

[52] The term "free" refers not to the price of a product but to "freedom". Many prefer to use the term "free/libre and open-source software" (FLOSS) to clear up the ambiguity. See Richard Stallmann, "FLOSS and FOSS", *GNU Operating System*, available at: www.gnu.org/philosophy/floss-and-foss.en.html.

[53] Albeit still being subject to licenses. See, for instance, Open Source Initiative, "Licenses & Standards", available at: https://opensource.org/licenses; Janelia Farm FlyEM Project, "Open Source Licenses and Their Compatibility", available at: https://janelia-flyem.github.io/licenses.html.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

propose changes that leave a backdoor in the software,[54] as mentioned above with reference to Birsan's study. Moreover, the amount of support and security that can be provided for FOSS often depends on the size and expertise of the contributing open-source community.

A complementary concept to open hardware and open-source software is open standards. Open standards are standards that do not prohibit the creation of conforming open-source implementations.[55] Open standards in turn give open-source implementations the guidance and interface specifications needed to be portable and interoperable.[56] Even beyond FOSS, open standards can prevent vendor lock-in, simply because they are not proprietary and can be used by other vendors as well.[57] The Internet Engineering Task Force (IEFT),[58] with the help of other organizations, produces and maintains many open standards in so-called Requests for Comments (RFCs). RFCs are a series of documents that contain technical and organizational notes about the Internet; some of them become standards.

When open standards or open-source alternatives to proprietary solutions are not available or not satisfactory, diversifying the digital supply chain can reduce the impact of vendor dependence and improve overall supply chain resilience.[59]

The ICRC and "cyber crossfire"

The risk of "cyber crossfire" for a neutral, impartial and independent humanitarian organization like the ICRC, within the global competition between the great powers, has been mentioned above. In the area of supply chain attacks, it involves the risk of an organization becoming a victim of collateral damage, or having its systems exposed to attacks targeted at a different entity, due to its reliance on the same digital supply chain as that of the target of the operation. In the physical world, the ICRC would not open an office close to a military installation because military installations are obvious (and under certain conditions lawful) targets for enemy forces in armed conflicts. In the same vein, in the digital world, risk assessment for digital procurement should consider the risk of suppliers, or a particular piece of software or hardware, being targeted because they are used by other customers, who may be (lawful or unlawful) targets of cyber operations.

[54] Ravie Lakshmanan, "PHP's Git Server Hacked to Insert Secret Backdoor to Its Source code", *The Hacker News*, 28 March 2021, available at: https://thehackernews.com/2021/03/phps-git-server-hacked-to-insert-secret.html.

[55] "What Are Open Standards?", *Opensource.com*, available at: https://opensource.com/resources/what-are-open-standards.

[56] Jon Siegel and Richard Mark Soley, "Open Source and Open Standards: Working Together for Effective Software Development and Distribution", *Technology Innovation Management Review*, November 2008, available at: https://timreview.ca/article/207.

[57] Andy Gower, "Open Standards vs Open Source: A Basic Explanation", IBM, 2 April 2019, available at: www.ibm.com/blogs/cloud-computing/2019/04/02/open-standards-vs-open-source-explanation/.

[58] See the IEFT standards and mission, available at www.ietf.org/standards/ and www.ietf.org/about/mission/ respectively.

[59] Sarah Hippold, "Diversifying Global Supply Chains for Resilience", Gartner, 4 February 2021, available at: www.gartner.com/smarterwithgartner/diversifying-global-supply-chains-for-resilience/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

This may be an element to militate for a more "independent" supply chain, or a supply chain that has less dependencies and therefore provides its users with more "sovereignty".

On the other hand, suppliers who serve other customers, including customers active in regulated business sectors or business sectors involving sensitive information handling, or who handle critical infrastructure, such as suppliers offering public cloud services, may be more likely to have very high security measures in place – even if the SolarWinds hack proved that this is far from a straightforward assumption.[60] Ultimately, therefore, the choice of supplier and supply chain for an impartial humanitarian organization may need to take into account, in addition to all the elements listed in the section above, a trade-off between the benefit of enjoying the alleged higher security standards of "industrial" suppliers and the risk of cyber crossfire.

The assessment of digital supply chain risks, therefore, starts by identifying the potential threats and threat actors that apply specifically to each individual organization, and by analyzing the available mitigating measures in respect of each of those threats and threat actors. Threat actors range from unskilled actors who take advantage of well-known, unpatched software vulnerabilities through ready-to-use exploitation tools,[61] to States and State-sponsored groups with access to zero-day exploits,[62] the ability to interfere with products of vendors under their jurisdiction[63] and even the resources to combine cyber tools with human intelligence.[64]

In analyzing how to address risks arising from each of these threat actors, it may be established, for example, that the impartial humanitarian organization in question is not specifically on the radar of "script kiddies", and the organization, vis-à-vis those actors, is in neither a better nor a worse position than any company trying to protect itself from them. Yet the more limited capabilities of these threat actors may mean that the risks represented by them may be adequately addressed with state-of-the-art cyber hygiene, whether in an "industrial" and allegedly more secure supply chain or in a more "independent" or "sovereign" supply chain. On the other hand, as far as more capable threat vectors such as State or State-sponsored attackers are concerned, it may not be possible to effectively defend an organization from attacks originating from them if they really invest resources into developing an attack.

[60] David E. Sanger, Nicole Periroth and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm", *New York Times*, 28 May 2021, available at: www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[61] Alpine Security, "7 Steps to Hack a Target with Virtually No Experience", available at: https://alpinesecurity.com/blog/7-steps-to-hack-a-target-with-virtually-no-experience/.

[62] Project Zero, "Introducing the In-the-Wild Series", available at: https://googleprojectzero.blogspot.com/2021/01/introducing-in-wild-series.html.

[63] Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice", *CNBC*, 4 Match 2019, available at: www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[64] David Kushner, "The Real Story of STUXNET", *IEE Spectrum*, 26 February 2013, available at: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

The ICRC can, however, leverage a number of unique protection assets that other organizations do not have, such as public international law relating to international organizations,[65] international humanitarian law,[66] and – beyond what is provided under international humanitarian law in times of armed conflict – the respect by all States for the neutrality, impartiality and independence of the organization and the respect for the solely humanitarian nature of its work, as enshrined, for example, in Article 2 of the Statutes of the International Red Cross and Red Crescent Movement.[67] The ICRC can thus leverage its widespread acceptance and the protection it enjoys under the provisions mentioned above, also in the digital world; however, there are two essential preconditions for this.

The first precondition, just as would be the case outside the cyber paradigm, is the fact that a humanitarian organization needs to be capable of credibly anticipating, detecting (ideally preventing) and, very importantly, understanding who is responsible for possible adverse cyber operations likely to affect the organization. The challenges around attribution are many, and very significant.[68] In public discourse, attribution of cyber operations is often associated with public attribution by States, accompanied, in many cases, by State responses such as sanctions and indictments. There are several reasons why States use public attribution as a key part of an integrated national security policy response.[69] This State-specific angle is outside of the scope of this article and is analyzed in detail elsewhere.[70] What matters, in the framework of the present analysis, is not so much attribution as such, but the capacity for an organization to identify the likely source of an adverse cyber operation, as a necessary condition to enable the organization to continue its bilateral confidential dialogue with its interlocutors[71] – simply put, to allow the organization to know who to talk to. From the angle of an actor that may be considering directing an operation against a humanitarian organization, this is also likely to have a deterrent effect, since that actor will know that the operation will not go undetected. Beyond identification of the origin of a cyber operation as an enabler of bilateral confidential dialogue, public attribution by States concerning an operation affecting the ICRC can also have a significant deterrent effect, as it can put the

[65] "Scenario 04: A State's Failure to Assist an International Organization", *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_04:_A_State's_failure_to_assist_an_international_organization.

[66] Tilman Rodenhäuser, "Hacking Humanitarians? IHL and the Protection of Humanitarian Organisations against Cyber Operations", *EJIL: Talk!*, 16 March 2020, available at: www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.

[67] Statutes of the International Red Cross and Red Crescent Movement, Adopted at the 25th International Conference of the Red Cross and Red Crescent, Geneva, 1986 (amended 1996 and 2006), available at: www.icrc.org/en/doc/assets/files/other/statutes-en-a5.pdf.

[68] Florian J. Egloff, "Public Attribution of Cyber Intrusions", *Journal of Cybersecurity*, Vol. 6, No. 1, 2020.

[69] *Ibid.*, p. 3.

[70] *Ibid.*

[71] ICRC, "The International Committee of the Red Cross's (ICRC's) Confidential Approach: Specific Means Employed by the ICRC to Ensure Respect for the Law by State and Non-State Authorities: Policy Document", *International Review of the Red Cross*, Vol. 94, No. 887, 2012, available at: https://international-review.icrc.org/sites/default/files/irrc-887-confidentiality.pdf.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press

spotlight of the international community on conduct that would likely attract significant stigma, and that may in some circumstances amount to a violation of international law. In other words, and again, the basis for the security approach outlined above is based on deterrence deriving from the fact that if a hack is attempted, it will not go undetected, and the perpetrator will be identified.

The second precondition is the capacity to carry out in cyberspace the same extensive work of prevention, dissemination and dialogue with weapons bearers that the ICRC leverages in the physical world in order to build trust and acceptance, and ensure access. This, in turn, requires a clear mapping of the different types of weapons bearers operating in this space, and an understanding of their drivers, objectives, motives and control structures (or lack thereof).[72] From this standpoint, a risk mitigation plan would clearly include the development of technical and organizational solutions for ensuring that digital assets belonging to an impartial humanitarian organization, or otherwise used to deliver humanitarian assistance, could be clearly marked and identified as protected.[73]

Conclusion

Despite the lack of an easy solution, the question of supply chain security remains an important one. The reaction to attacks of the SolarWinds type should not be defeatist, and should instead be to ask: how can we manage and mitigate our dependency on these supply chain systems that have put us in such vulnerable positions in the first place?

The purpose of developing a cyber security strategy should include looking beyond what can be achieved today and tomorrow and identifying areas of possible investment, disinvestment, organizational changes and partnerships, with a clear vision of the landscape in which the organization may find itself in five to ten years both in terms of specific threat actors and the resources and means to deal with them. It is suggested that any strategic decision that considers an organization's unique security assets is one that better enables the organization to deliver on its mandate and mission.

In this sense, what is therefore required is a careful strategy around digital sovereignty, intended, as discussed above, as a careful and deliberate management of the organization's digital dependencies and over-dependencies according to its unique security assets. Such a strategy could involve investment in moving the cursor towards reducing dependencies to the maximum extent that is possible and meaningful, and evolving in an incremental way in this direction over time.

[72] M. Marelli, see above note 29.

[73] See, for example, Felix E. Linker and David Basin, "Signaling Legal Protection during Cyber Warfare: An Authenticated Digital Emblem", *Humanitarian Law and Policy Blog*, 21 September 2021, available at: https://blogs.icrc.org/law-and-policy/2021/09/21/legal-protection-cyber-warfare-digital-emblem/; Antonio De Simone, Brian Haberman and Erin Hahn, "Identifying Protected Missions in the Digital Domain", *Humanitarian Law and Policy Blog*, 23 September 2021, available at: https://blogs.icrc.org/law-and-policy/2021/09/23/protected-missions-digital-domain/.

https://doi.org/10.1017/S1816383122000194 Published online by Cambridge University Press