zif Center for International Peace Operations

100 Voices on Technology & Peace Operations

Managing cyber security in peace operations

The future of cyberspace – a domain for conflict or collaboration?

01 September 2020 | Kaja Ciglic & John Hering

Increased reliance on digital technology has had a tremendous transformative effect. While there are clear advances with regard to digital collaboration and exchange, Cyberspace has quietly emerged as a distinct "fifth domain" of conflict over the last 20 years – affecting developed and developing, conflict-ridden and peaceful societies alike. Rules of engagement are urgently needed but difficult to agree on – not least because the transnational nature of cyber threats is at odds with traditional state-to-state mechanisms of negotiation and decision-making. Recent attacks have led to some momentum in this process, but to be effective and sustainable international governance architecture needs to be revamped to include a wider spectrum of stakeholders in new systems and structures.

The world has changed dramatically since the turn of the century. Geopolitical alignments and power centers have shifted, the global economy has been a rollercoaster of highs and lows, and we have become acutely aware of the impact humanity has had, and continues to have, on our shared climate. However, no one thing has had a more transformative effect during this time than our increased reliance on digital technology. It has disrupted existing business models and introduced new employment frameworks. It has fundamentally changed how we live our daily lives. The Covid-19 pandemic has brought this impact into even sharper focus. In recent months, while we have learned how to socially distance, we have also come to embrace digital technologies like never before. Seemingly overnight, this technology became the lynchpin to working remotely, maintaining relationships, studying and learning, as well as to advancing groundbreaking medical research at breakneck speed.

THE RAPIDLY AND QUIETLY GROWING "FIFTH DOMAIN" OF CONFLICT

Perhaps unsurprisingly, as more human interaction has moved online, there are increasingly those who seek to take advantage of our increased reliance on technology. In the 21st century, Cyberspace has quietly emerged as a distinct "fifth domain" of conflict. It is characterized by the same geopolitical tensions and competition present in the other domains – land, sea, air and space – where nation states jockey for position by undermining adversaries, improving defenses, and

rarely ceding advantages. However, due to the hidden nature of the cyber domain, conflict online has continued to escalate without garnering public attention or dominating headlines, despite becoming increasingly commonplace, and increasingly damaging. And while not always as immediately destructive as a kinetic attack, cyberattacks has shown the potential to be just as devastating.

While much of today's conflict online flies under the radar, unnoticed, there have been seminal events that have pierced public consciousness as the world sleepwalked into the cyberwar era. For many, the event that marked the onset of this era occurred in 2007, when an announcement that Estonia planned to move a Soviet war memorial precipitated a vicious cyberattack in response that knocked banks and government services offline. Three years later, the Stuxnet worm demonstrated that malware can have an impact on the physical world as well, covertly ruining nearly one-fifth of Iran's nuclear centrifuges. However, it was in 2017 when the world suddenly realized that cyberattacks will not always be constrained to a specific location as part of a particular military or policy objective, and that the collateral damage can be catastrophic.

In May of 2017, the WannaCry ransomware attack quickly spread around the world, crippling computer systems in over 150 countries and causing billions of dollars in damages in a matter of hours before finally being stopped thanks to a miraculously discovered "kill switch". However, a mere month later, government agencies and businesses in Ukraine were taken offline by the Notpetya attack – which again spread around the world with merciless speed. And this time there was no kill switch, just massive losses. The White House estimates the total damages of this single attack to be more than $10 billion. However, as you can see in this video, the impact of such an attack extends well beyond financial loses alone, and is particularly painful when they include essential services like healthcare.

FLATLINING – CYBERATTACKS IN A PANDEMIC

Unfortunately, the lesson that was learned from the WannaCry attack was not that cyberattacks on hospitals should be banned. Instead, in the midst of today's global pandemic, we have seen news reports of criminal and nation-state attacks targeting critical medical facilities – including Brno University Hospital in the Czech Republic, the Paris hospital system, the computer systems of Spanish hospitals, hospitals in Thailand, medical clinics in the U.S. state of Texas, a healthcare agency in the U.S. state of Illinois and even international bodies like the World Health Organization. Our teams at Microsoft have also detected and responded to attacks targeting the healthcare sector in many countries, and we know they are coming from both criminals as well as multiple nation states.

Microsoft has been vocal on the need for clearer rules of engagement in cyberspace for a number of years, calling in particular for the recognition and reaffirmation of the fact that international law applies in cyberspace, both in times of war and in times of peace. Recent attacks have finally galvanized a global multi-stakeholder community to join in this effort as well, calling for governments to take immediate and decisive action to stop all cyberattacks on hospitals, healthcare and medical

research facilities, as well as on medical personnel and international public health organizations. In May, nearly 50 business and government leaders from around the world, as well as humanitarians and Nobel Laureates, joined in signing a letter which underlined that just as we do not tolerate attacks on healthcare infrastructure in the physical world, we cannot tolerate such attacks in cyberspace. Prominent amongst those were organizations such as the CyberPeace Institute, International Campaign to Abolish Nuclear Weapons, International Committee of the Red Cross, as well as technology companies, and individuals who have seen first had the damage conflict can wring – both offline and online.

This sentiment has been echoed as well by the group of over 100 international law experts who joined in issuing a statement earlier this summer detailing how international law applies to online operations against medical facilities. This group has since followed up with a similar illumination of the legal protections available for vaccine research – a pressing topic, given recent reports of attempts to access information related to the search for a Covid-19 cure and vaccine. It is important to remember that these actions – while on the surface perhaps minor intrusions – have the potential to disrupt or harm the availability or integrity of research data and, in so doing, compromise the ability to conclude clinical trials, obtain approval for them or to manufacture or distribute eventual treatments.

BRINGING ORDER TO CHAOS – SEEKING RULES IN CYBERSPACE

We are hopeful that these statements from experts and leaders might galvanize governments into action. Of course, this is not a new area for states – neither in plotting offensive measures, nor in trying to stabilize the online environment. Discussions on this complex subject have been ongoing for more than a decade. The United Nations Group of Governmental Experts (GGE) on Advancing Responsible State behavior in Cyberspace in the Context of International Security (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security) is a UN-mandated working group that has been discussing these issues since 2004, in six different formations. In 2018, another UN-mandated working group – the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) – was established in parallel with the GGE and is open to 'all interested states'. Cybersecurity also features prominently in the Secretary General's Roadmap on Digital Cooperation, a first of its kind report and important recognition of importance of multi-stakeholder collaboration in the digital domain.

International negotiations and agreements, however, are slow moving instruments, especially when compared to the pace of technological developments. And it is not just geopolitics that bogs down progress. Traditional state-to-state dynamics are further complicated by the unique qualities of a digital domain where accountability and enforcement of rules are difficult. Attackers online can be hard to identify, and then even harder to associate with a particular government. And without geographical boundaries, every point of connectivity can also be a border with determined adversaries – making it difficult to define the parameters of acceptable behavior that allows governments to look after their legitimate national interests. Furthermore, governance of a digital

100 Voices on Technology & Peace Operations

landscape has been formed, and continues to evolve, with private sector leadership and bottom-up innovation, demanding close coordination between governments and the technology industry.

We have seen examples for the technology industry that seek to not only push governments to towards clearer rules of behavior, but the technology sector itself. One prominent example is the Cybersecurity Tech Accord, an alliance of over 140 companies committed to promoting a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats. In particular, the group is aligned around four foundational principles:

1. Strong defense: Everyone deserves equal protection online irrespective of technical acumen, culture, location or motive for any malicious attack.

2. No offense: Companies are committed to not knowingly undermining the security of the online environment, and to protecting against efforts to tamper with our products and services.

3. Capacity building: Cybersecurity is a shared responsibility and companies will work to improve both the ability of everyone to act securely and safely online and the diversity of the security practitioner community.

4. Collective response: Companies know that they can achieve more together and will partner within the group and more broadly to address critical cybersecurity challenges.

These principles help guide the individual behavior of companies, stand as a badge of honor to ensure clear lines are drawn as to what behavior should be out of bounds, and overall improve the security of our common online ecosystem.

To protect the stability of cyberspace and push back on untenable and escalating trends will require clear rules and accountability. We therefore desperately need to not only bring this conflict out of the shadows and ensure the general public understands its potential impact, we also need to get governments to agree to limit their actions – even against some immediate self-interests – for our collective benefit. Most importantly, we need to revamp the existing architecture of international governance to ensure it is ready and up to the task for the challenges of a 21st century where life, business, and diplomacy are becoming fully digitized and the lines between them increasingly blurred. It also means including the right set of stakeholders in new systems and structures to create meaningful and enforceable expectations for a sustainable cyberspace.

And we need to act immediately. Otherwise, we are left to ponder, as United Nations Under-Secretary-General Fabrizio Hochschild did in his essay a few months ago, "how can we ask our health care workers, diagnostic and treatment facilities, researchers, and hospitals — those bound by the selflessness of duty and banded together against a common, hidden enemy — to continue containing the crisis while questioning whether vital equipment may be affected or shut down by a digital attack?"

100 Voices on Technology & Peace Operations

ABOUT THE AUTHORS

Kaja Ciglic leads Microsoft's work on digital peace, focusing on encouraging international peace and stability online. Previously, she worked on the company's international cybersecurity policy work. Before joining Microsoft, Kaja led the APCO Worldwide's technology practice in Seattle, and worked as a director in APCO Worldwide's Brussels office. She holds a BSC in international relations and history, and a MSC in European politics, both from the London School of Economics.

John Hering is a Digital Diplomacy and Cybersecurity Business Program Manager at Microsoft. He analyzes the global cybersecurity landscape, drives engagement across geopolitical boundaries and contributes to Microsoft's efforts to promote peace and security in cyberspace through various multi-stakeholder initiatives. digital attack?"