Behavioral norms in cyberspace

Can corporations make the digital sphere secure?

BY MYRIAM DUNN CAVELTY AND JACQUELINE EGGENSCHWILER

Not so long ago, when it came to cyberspace, states were believed to be powerless entities with no meaningful policy tools at their disposal. The supposed novelty of the cyber domain was thought to render traditional forms of state intervention and strategies useless. Now researchers and policymakers have come to realize that this is not the case, and that the erroneous assumptions of sovereign powerlessness were the result of flawed arguments inspired by technological determinism. Cyberspace is not a natural environment that has developed beyond the point of human control. On the contrary, it is man-made and almost entirely malleable.

As states have come to reveal themselves as capable and determined actors, willing to use and shape the digital realm as part of their strategic and military toolsets, unease over the escalatory potential of offensive cyber operations has risen. States have invested heavily in digital infrastructures and have built up cyber-command units, often at the intersection between military and intelligence branches. Concurrently, terms such as cyberwar, cyberweapons, or cyber arms race have entered the vocabulary of policy analysts and commentators, and the latter seem to agree that in classic security-dilemma fashion, levels of insecurity have increased rather than decreased.

Through their actions, great powers reveal themselves as able and willing to use and shape the cyber domain as part of their strategic and military toolbox. Therefore, the sense of unease about the escalatory potential of cyber operations is certainly not waning. The overall feeling is that the problem has gotten worse in both quantity and quality. Many experts refer to the malware used in some operations as cyberweapons and regard the build-up of cyber capabilities by state actors as part of a cyber arms race. The uncertainty over the intentions of other states leads to heightened feelings of insecurity and, again in classic security-dilemma fashion, to high incentives to build up (offensive) capabilities and cyber-command units, often at the intersection between the military and intelligence.

The uncertainty about the intentions of other actors and general unease about offensive cyber capabilities cause states to control the risk of escalation and fallout. As a result, the number of ministerial meetings and conferences attempting to agree on norms of responsible behavior in the virtual realm has increased. However, with global political tensions on the rise and cyberspace being treated as a strategic domain, the chances of agreeing on anything meaningful are close to zero. The failure to arrive at a consensus document by the 2017 United Nations Group of Government Experts (UN GGE), which was tasked with examining extant and nascent threats derived from the digital realm, is one case in point. The ideologically inspired bifurcation of the UN-driven norms process is another.

However, because cyberspace is of strategic importance for a great variety of different actors, state behavior, including the failure to come to an agreement concerning rules of the road for the virtual realm, does not go unchallenged by other stakeholders. Subsequent to the UN GGE's inability to come up with a consensus report, and following major cybersecurity incidents of transnational magnitude, including WannaCry and Petya/NotPetya, there has been a surge in the number of private-sector initiatives directed at fostering responsible conduct in the digital domain. Examples include Microsoft's proposal for a Digital Geneva Convention as well as its adoption of a Cybersecurity Tech Accord, Google's New Legal Framework for the Cloud Era, Siemens' conclusion of a Charter of Trust as well as Telefónica's Manifesto for a New Digital Deal.

From an empirical perspective, it is fair to say that in cyberspace, the definition of norms is no longer just the domaine réservé of nation states, but increasingly also the purview of business enterprises. Private actors extend their traditional zones of operation and engage in diplomatic dealings at an international level. While the key drivers for corporate engagement on issues relating to international security and stability in cyberspace may be commercial in nature, i.e. the reduction of costs and risks or the acquisition of competitive advantage, the private-sector proposals also display considerable degrees of normativity which go beyond pure business interests and are likely to have an impact on international politics.

Not only have private companies come to assume roles as proposers of norms and diplomatic change agents, they have also put on the table important topics that were previously unaddressed. Most of the normative efforts conducted by states are geared towards the high-end form of cyber aggression, the fabled cyberwar, which could be devastating but presently has a very low probability of occurrence. Indeed, more common are destabilizing cyber acts below the threshold of war. The biggest actual cyber issue, next to cybercrime, is cyber exploitation or cyber espionage, with the goal of gathering classified information from an adversary and using it in strategically opportune ways. This is the world of intelligence agencies, whose actions are regulated by domestic law in their home states but remain more or less unconstrained by international law.

The private-sector initiatives aim to tackle the destabilizing actions of intelligence agencies. Bad actors who plant and exploit vulnerabilities in current operating systems and hardware are making cyberspace more insecure; their aim is to have more access to data while preparing for future conflict. Backdoors and unpatched vulnerabilities reduce the security of the entire system – for everyone. In short, the strategic exploitation of vulnerabilities in computer systems and the weakening of encryption standards have the potential to destroy trust and confidence in cyberspace overall, which would produce considerable economic and social costs.

While the emergence of a coherent global cybersecurity regime in the near future is unlikely, a push for more state restraint and responsible behavior by private-sector protagonists seems probable. In the best case, corporate pushback, especially if coupled with technical innovation and better cybersecurity solutions, will lead to a more-or-less deliberate change in the conduct of state actors. While the norm-building activities of private-sector entities raise a number of important follow-up questions pertaining to legitimacy and order, in the worst case they will create pressure for states to continue diplomatic efforts to make cyberspace more – not less – secure.

MYRIAM DUNN CAVELTY
is a senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS).

JACQUELINE EGGENSCHWILER
is a PhD student at the University of Oxford's Centre for Doctoral Training in Cybersecurity and the Faculty of Law.

Fail-safe cyber resilience

We need early warning and quick response systems that work

BY TOM KOEHLER AND OLIVER ROLOFS

The unprecedented scale of digital conversion and very high level of connectivity in the world around us drastically increase the scope for cyberattacks. One undeniable result of this fact is the increased vulnerability of all sectors of industry, defense and critical infrastructures as well as our private lives around the globe. Living in the era of digital dependency has obviated the need to emphasize that a cyberattack on any of these critical sectors could spell disaster for national security, our work and the safety of our citizens. As we face a new technology wave driven by the rise of 5G networks, artificial intelligence and billions of devices in the internet-of-things, we can be sure that our exposure to attack will only grow.

SHUTTERSTOCK

"Someone sitting on their bed that weighs 400 pounds" – or Guccifer 2.0.

Who would have believed, just a decade ago, that the internet would enable cybercrime to inflict almost $600 billion worth of damage around the world in 2018? Or that social media could be misused as systems of mass disinformation, and thus significantly affect the outcome of elections? And who can imagine today that blockchain technology has the potential to bring entire economic systems grinding to a halt?

Although we are increasingly aware of the risks involved in these new emerging technologies, the actual use of the technologies themselves is never a matter of debate. This points to the fact that we urgently need a paradigm shift in security policy. Security in the digital era is much more than an inconvenient cost factor or a field of action for technology freaks. It is something we have a pressing need for if we are to build sustainable cyber resilience into the potentials offered by digitalization. And it should play a role not only at the highest level of government, but also in the cities where we live.

Urbanization is proceeding apace. Experts forecast that more than two-thirds of the world's population will live in cities by 2050. Urbanization is accompanied by far-reaching technological change that is increasingly encroaching on our lives. We are already living in a world that has seen itself transformed into a global village by digitalization. And this process is set to continue. If our cities are to keep pace with future needs and not end up drowning in dirt and trash, they must and they will become smart cities. In the future, sustainable urban development is going to need modern information and communication technologies to be applied in urban management more than ever before. But how does the process of digitalization actually work in practice?

Generally speaking, the digitalization of a city takes numerous previously isolated systems and brings them together. Homes and buildings can suddenly communicate with utility companies and garbage disposal services. Traffic lights are digitally connected to cars and public transit vehicles. Hospitals might access data from primary care providers and health insurers to optimize their demand planning.

It is precisely this process of connecting up different data systems that carries the greatest security risks, because the highly dynamic system of systems that emerges as a result of all this digital connectivity will not ordinarily have any organic protection built into it in the design phase. It is frequently not until later that additional interfaces are developed to integrate security systems, and this is exactly where technology strategy risks emerge, many of which we are not even aware of and must better understand. At present, we are enormously trusting of new technology, whereas our understanding of risk is still limited.

We overestimate our capacity for control and we often underestimate the risks. For many of the things in life, we have developed effective ways of making decisions that keep us out of danger. But we still lack such rules of thumb for life in the digital age.

But what happens if one day hackers target an entire city or a country's entire power grid? How well prepared are we today to withstand a complete digital meltdown?

Without a doubt, more internet users, devices, connections and data flow mean that the risks will continue to grow and, in particular, to burden our critical infrastructures. At the same time, there are considerable concerns that we are neither prepared to handle these threats nor able to rely on fallback options. Indeed, we lack the capacity to even respond in the event of a large scale cyberattack. States, cities and their industries still fail to recognize that they are all potential targets for cyber attacks.

In real life, crises do not run on a timetable, and they are not linear. Cyber-risk resilience questions need to be answered in the here and now. And they must be answered for every government at a national and local level as well as for companies that work with digital processes and administrative structures, because it will not be possible to provide overarching cybersecurity and cyber-risk resilience. Instead of focusing only on resisting cyberattacks, organizations must look at how they can be more resilient.

As unwelcome as this message may be to a risk-averse society, we must learn to manage these threats and develop functioning fallback options and cyber-resilient capabilities in case of large-scale cyberattacks. We need to work on increasing people's awareness of cyber resilience in order to build organizational capabilities to sense, resist and react to disruptive cyber events, and to recover from them in a timely fashion.

While national crisis management exercises are necessary, local urban infrastructures also need to be more effectively prepared to engage in interconnected civil defense against cyberattacks – the threat is real. Just look at the digitally progressive country of Estonia. In 2007, the Baltic state spent weeks being subjected to the largest cyberattack in history, which was waged by neighboring Russia. In order to better protect itself in the future, Estonia subsequently developed agile defense and resilience strategies with national and international backup strategies.

Germany recently heeded this example by starting to build up a cyber reserve within the German armed forces. The civil mobilization of cyber experts in a crisis – i.e. specialists who can return the country to a state of normalcy after an attack – is a commendable first approach.

Aside from mobilization, however, we need to improve the orchestration competency between all levels of governments, including local authorities, so that a form of continuous, citizen-centric cyber-risk resilience can be realized in the future. But this is precisely where we find that the majority of policymakers are not sufficiently sensitized to the subject or remain rooted in old patterns of thinking.

In today's world, digitalized infrastructures are crucial to the success of planned urbanization. Without a doubt, there is added value to be had from managing a city digitally through connected and optimized infrastructures and services. However, for this kind of urban planning and management to be possible, cyber security and resilience strategies must become more agile and should be a crucial part of the plan from the very beginning.

Resilience includes both early warning and quick response systems, as well as efficient procedures to prepare our urban societies and their businesses. Having functioning and sustainable fallback options and resilience capabilities are key in the event that network-based infrastructures are targeted in an attack. In this light, we must rethink cybersecurity and stop ignoring the digital elephant in the room.

To achieve our goal of fail-safe cyber resilience, we need to engage in permanent and interdisciplinary dialogue with more clarity and with concrete actionable recommendations. We must take an innovative hands-on approach that creates adequate cyber resilience while at the same time not restricting our creativity and freedom. It goes without saying that organizational structures and cultures must also be adopted in order to cope with the dynamic and complexity outlined above. If local governments and their representatives understand these challenges and are successful in this endeavor, their citizens will feel more secure and understand that the risks do not outweigh the opportunities inherent in the new emerging technologies.

TOM KOEHLER is a founding partner and **OLIVER ROLOFS** a partner at connecting trust.