ICT for peace FOUNDATION 20 years

The future of cybersecurity policy lies in civil society

Julia-Silvana Hofstetter

Current geopolitical events are putting state actors and military capacities at the center of cybersecurity policy. At the same time, cyber experts are increasingly advocating a human-centered conception of cybersecurity that focuses on digital human rights and reconsiders the role of civil society actors and individual citizens in shaping cybersecurity policy. Even in armed conflicts such as Ukraine or Afghanistan, civil society actors represent an important complement to military structures when it comes to protecting the population against cyber risks (Buzatu 2022, Hofstetter 2024).

Will no one be safe in cyberspace in the future? We read about cyber attacks on our universities, hospitals and authorities. In the context of Ukraine, there is talk of the first real cyber war, i.e. an interstate conflict in which the use of cyber weapons plays a central role in warfare. This seems to reinforce the long-prevailing state- or business-centric conceptions of cybersecurity, which focus on national security or cybercrime. The state-centric perspective prioritizes military security interests and the protection of infrastructures deemed critical to the functioning of state-owned enterprises. The business-centric focuses on protecting companies from cybercrimes. At the same time, experts are increasingly warning against a militarized understanding of security in the digital space.

They advocate a human-centered cybersecurity policy in order to be able to do justice to the increasingly complex threat situation in the digital space and expand it to include new policy areas (Weekes 2018). This not only emphasizes the role of digital human rights, but also sees the opportunity to involve a broader field of actors. This is often referred to as "citizen co-production" (Chang et al. 2018) or a "whole-of-society approach" (Porche 2022). In an international context, too, a growing field of actors is committed to the global expansion of the "civil cyberdefense" infrastructure. Civil society actors are already helping NGOs, activists and journalists to protect themselves against cyberattacks. Even in armed conflicts such as in Ukraine or Afghanistan, they represent an important complement to military actors when it comes to protecting the population against cyber risks (Buzatu 2022, Hofstetter 2024).

Human-centric cybersecurity

A human-centered definition of cybersecurity emphasizes the direct impact of cyber threats on individuals rather than on states or companies, and thus also expands the circle of threat actors from non-state actors and foreign states to institutions of their own government. This represents a decisive shift in the distribution of roles between the individual and the state: on the one hand, the state itself can – intentionally or unintentionally – become a threat actor for its citizens. Conversely, individuals and non-state actors are no longer seen primarily as potential cybercriminals, but are at the center of the effort as the actual recipients of cybersecurity.

So, the human-centered approach emphasizes the cybersecurity needs and responsibilities of civil society (Kavanagh/Stauffacher). From this perspective, it is also evident that individuals experience cyber threats differently and that those who already belong to a vulnerable or marginalized group in society can also be disproportionately more affected by cyberattacks (Hofstetter/Zahn 2020). In addition, civil society organisations – as opposed to government institutions, private companies or the civilian population – are often forgotten in traditional cybersecurity considerations. Although they face the same or in some cases even stronger threats, they have far fewer resources to protect themselves. Under the slogan of a whole-of-society approach to resilience – i.e. a "whole-of-society approach" that goes beyond a mere cross-agency "whole-of-government approach" – some states are advocating the development of national cybersecurity instruments that take into account the needs of all affected social groups and compensate for resource inequalities between different sectors.

In addition to the protection of technical systems and infrastructure, a human-centered approach conceived for society as a whole also aims to build social resilience that goes beyond the purely technological and also includes human rights and democratic institutions as an object of cybersecurity policy worthy of protection. This not only makes it possible to better understand the complex threat situation in cyberspace – in which data privacy violations, digital disinformation, internet censorship, online violence and fair access to digital infrastructure must also be taken into account – but also to think of actors such as human rights activists and journalists as part of the critical infrastructure.

This makes it possible to conceptualize cybersecurity more holistically, addressing the technological, social and legal aspects together, without distinguishing between national security interests. The whole-of-society approach also makes it possible to consider citizens and civil society organisations as active participants in cybersecurity policy, which is "co-produced" by the state with the involvement of civil society. But what exactly does such active participation of civil society look like and why is it so crucial for a future-proof cybersecurity policy?

“A human-centered definition of cybersecurity emphasizes the direct impact of cyber threats on individuals rather than states or corporations, and thus also expands the circle of threat actors from non-state actors and foreign states to institutions of one's own government.”

State-mandated co-production

National Cyber Strategies (NCS) are among the most important instruments in shaping national cybersecurity and cyber foreign policy. They point the way forward for government efforts to anticipate the opportunities and risks of technological change. More than 100 countries worldwide have already introduced an NCS, including Switzerland, which published its new NCS in April 2023. In the formulation of the NCS, possible instruments for involving civil society include not only consultation processes but also more innovative formats such as online surveys among stakeholder groups or citizen participation through open forums organized throughout the country.

While many countries commit themselves to a multi-stakeholder approach when formulating their national cyber strategies, this approach is often limited to the involvement of the private sector, involving civil society only pro forma or limiting their participation again when it comes to the concrete implementation of the measures.

Globally, however, there are also positive examples: Belize, with the support of the Organization of American States, set up a multi-stakeholder NCS task force to formulate its 2020 strategy, which consisted of 15 different stakeholders from government, the private sector, civil society and academia and is also to accompany the implementation of the strategy. Sierra Leone's Ministry of Information and Communications, in turn, convened a multi-stakeholder dialogue for its latest NCS, in preparation for which it also offered workshops for civil society organisations to train them to take up their seats.

The Australian government organised a digital open consultation in 2020 as part of its NCS development, collecting feedback and publishing the over 100 contributions received from stakeholders and individuals online. In Colombia, the digital rights NGO Fundación Karisma took a particularly active role and, after initial resistance from the government, managed to bring issues such as critical vulnerabilities in public data infrastructures that it had discovered into the NCS, adopted in 2020, by organizing roundtables and publishing analyses, recommendations and blog series.

Citizens and civil society organisations can also take an active role in providing cybersecurity.

Co-production on cybersecurity is not limited to the design of cybersecurity policy policy documents or a more inclusive mapping of cybersecurity needs: citizens and civil society organisations can also take an active role in providing cybersecurity. Many countries are already trying to make use of civil society resources, for example by setting up cybercrime and online violence hotlines, by contracting civil society organisations for campaigns to raise public awareness of cybersecurity risks, by deploying hackers to stress test critical infrastructures, or by involving volunteers in cyberdefence military structures. Estonia, for example, founded a voluntary cyber army unit called the Defence League Cyber Unit in 2010. It is a civilian entity integrated into the Estonian military, consisting of experts from the public and private sectors who can be called upon to provide support in times of a cyber crisis. Another example is the recently created volunteer "IT army" of Ukraine.

Unlike in Estonia, where the volunteer army is used only for defensive purposes and in clearly institutionalized hierarchies, the ad hoc Ukrainian IT army is also involved in offensive operations. The members who work with Ukraine's Ministry of Digital Transformation are diverse, ranging from IT experts and former military personnel to social media influencers (Soesanto 2022).

Civil-Cyberdefense

In addition to state-mandated co-production, in which civil society actors and civilians are involved in the design and implementation of state measures, the concept of "civil cyber defense" is also becoming increasingly important in times of peace and crisis.

Specialised civil society Actors support NGOs, activists and journalists in protecting themselves against cyber risks. They provide guidelines and training on how civil society organizations and activists can improve their digital security practices. For example, they offer rapid emergency assistance in the event of cyberattacks, such as the NGO Access Now with its "Digital Security Helpline" or the Cyberpeace Builders Program of the Cyberpeace Institute, a volunteer program consisting of a global network of cybersecurity experts from the private sector.

In addition to international NGOs, universities are also increasingly active in the field of civil cyberdefense. In so-called cybersecurity clinics, universities such as UC Berkeley, which is also part of the international network "Consortium of Cybersecurity Clinics", train student teams: The aim is to support civil society organizations and other institutions that are part of the critical public infrastructure but have insufficient resources for cybersecurity precautions (e.g. small hospitals or local governments) to improve their cybersecurity practices. security, defend against cyberattacks and advocate for their digital rights.

An active role of civil society outside of state-mandated co-production is particularly important in contexts in which the state itself becomes a threat actor and wherever state resources and competencies are not sufficient – for example, when national security interests such as the fight against terrorism are valued more highly than individual data protection rights, vulnerabilities in digitized public services are not taken into account sufficient care is taken when repressive states have their citizens and political opponents digitally monitored or countered with online violence.

Transnational cooperation in cyber crises

In international cybersecurity policy, which is mainly negotiated in multilateral cyber diplomacy forums of the UN and is mostly limited to the debate on intergovernmental norms of conduct in the digital space, the voices of civil society actors are still not heard enough. However, current examples of armed conflicts, such as the Taliban's takeover of Afghanistan, show how civil society actors step in in crisis situations and protect the population in cyberspace, where states and the international community do not yet have institutionalized solutions in place.

In international cybersecurity policy, which is mainly negotiated in multilateral cyber diplomacy forums of the UN and is mostly limited to the debate on intergovernmental norms of conduct in the digital space, the voices of civil society actors are still not heard enough.

Following the withdrawal of coalition troops from Afghanistan in 2021, many feared that the Taliban would gain access to the vast amounts of data and biometric registration technologies used by various international and national governments over two decades. There was concern that the Taliban would use this data to identify and track Afghans who had previously worked with foreign forces or the former Afghan government. Thousands of Afghans have also been forced to delete their online identities, digital footprints and social media data, fearing that the Taliban could use them to identify enemies of the regime. Regional and international civil society networks played a decisive role here.

Organizations such as Access Now, the Digital Rights Foundation, and Human Rights First set up helplines for Afghans who wanted to cover their digital tracks and avoid biometric surveillance. For example, guidelines from social media companies on deleting digital profile data have been translated into local languages (Hofstetter 2024).

Cybersecurity policy of the future – protection for whom and from whom?

A future-oriented cybersecurity policy must not only reassess civil society as the object and agent of such measures, but also deal more deeply with the question of whose security needs have been prioritized and forgotten in conventional cybersecurity considerations so far – in peacetime as well as in war. Cyberattacks on critical infrastructure in Ukraine, for example, are not limited to military structures and energy supply systems.

Journalists and human rights defenders have also fallen victim to cyberattacks and are increasingly reliant on international support to secure themselves and the sensitive data they work with. If you take a differentiated look at cyber threats for particularly vulnerable population groups, it also becomes clear that cybersecurity needs to be thought of more broadly. In the context of the Ukraine war, it has been reported how online platforms and social media groups in which civilians offer emergency aid to Ukrainian refugees have been misused as "Tinder" for human traffickers (Townsend 2022).

The central advantage of human-centered cybersecurity policy is that it raises the questions: Cybersecurity for whom – and above all: from whom? Not only in Afghanistan, but in the face of global autocratization in general, the question arises with regard to international cooperation in the cyber domain as to whether the digitalization of public services and infrastructures must not also be accompanied by an acceleration of the digital self-determination and defense of citizens and whether the strengthening of transnational civil cyberdefense infrastructures should be a focus – instead of autocratic states inadvertently giving them expertise and technologies that they could use for the digital repression of their own population.

This Article was first published in German language in swissfuture Nr. 04/23

References

Kavanagh C. Stauffacher D. (2014): A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security. ICT4Peace Foundation.https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2104-A-Role-For-Civil-Society.pdf

Chang, L. Y., L. Y. Zhong, und P. N. Grabosky (2018): *Citizen co-production of cyber security: Self-help, vigilantes, and cyber- crime,* in: Regulation & Governance, 12(1), 101–114.

Deibert, R. J. (2018): *Toward a human- centric approach to cybersecurity,* in: Ethics & International Affairs, 32(4), 411–424.

Weekes, B. (2018): Digital Human Security 2020**.** Human Security in the Age of AI: Securing and Empowering Individuals. ICT4Peace Foundation. https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2018-Digital-Human-Security.pdf

Hofstetter, Julia (forthcoming 2024): *Data Weaponization in Armed Conflict: A Gendered and Postcolonial Analysis of Afghanistan,* in: Alexis Henshaw und Anwar Mhajne (ed.): ‹Critical Perspectives on Cybersecurity: Feminist and Post- colonial Interventions›. Oxford University Press.

Hofstetter, Julia and Nicolas Zahn (2020):
Covid-19 and conflict prevention: When the stigmatisation of minorities and digital misinformation leads to outbreaks of violence. In: Neue Zürcher Zeitung (NZZ). https://www.nzz.ch/meinung/ covid-19-and-violent-conflicts-consists-in-the-stigmatization-of-minorities-and-the-dissemination-of-digital-falsification-information-the-actual-danger- ld.1584877?reduced=true

Porche, I. (2022): Cybersecurity needs a whole-of-society effort. The Hill. https:// thehill.com/opinion/cybersecuri- ty/3503303-cybersecurity-needs-a-whole- of-society-effort/

Soesanto, S. (2022): *The IT army of Ukraine: Structure, Tasking, and Ecosystem,* in: CSS Cyberdefense Reports.

Townsend, M. (2022): UK’s Homes for Ukraine scheme risks operating as ‹Tinder for sex traffickers›, say charities. The Guardian. https://www.theguardian.com/ uk-news/2022/mar/26/uk-homes-for-ukraine-scheme-risks-operating-as-tinder-for- sex-traffickers-say-charities

Buzatu, A. (2022): From Boots on the Ground to Bytes in Cyberspace: A Mapping Study on the use of ICTs in Security Services by Commercial Actors. ICT4Peace Foundation. https://ict4peace.org/wp-content/uploads/2022/09/ICT4Peace_Mapping_Study_ICTs_PSCs.pdf

Julia-Silvana Hofstetter is a political scientist and researches the role of new technologies in international peace and security policy. She is a Senior Advisor at the ICT4Peace Foundation, a Non-Resident Fellow at the Center for Long-Term Cybersecurity at UC Berkeley, co-director of the Peace & Security program of foraus – Forum Aussenpolitik, and President of Women in International Security Switzerland. Previously, she worked for Chatham House, the Center for Security Studies at ETH, the Geneva Center for Security Policy and the Federal Department of Foreign Affairs. She was also a 2021 WIIS Global NextGen Fellow for Cybersecurity & Gender. As an independent researcher, she advises organizations such as the ICRC, NATO, and the U.S. Department of State on digital peacebuilding, humanitarian data management, and feminist cybersecurity policy.

julia-silvana.hofstetter@graduateinstitute.ch

Keywords: cyber security, cyber diplomacy, cyber war, digital human rights, data privacy, civil cyber defence, civil society engagement, new technologies, human-centred

Geneva, 26 March 2024