RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0054

Wanted: Nobel Peace Price Winners Who Create Peace in Cyberspace

Wolfgang Kleinwächter

The paper starts with the statement that for the future of mankind cybersecurity is as important as the management of climate change. Building a global cybersecurity architecture should be a priority for diplomacy in the digital age. The paper covers the three main intergovernmental cybersecurity negotiation platforms: 1. The "Open Ended Working Group" (OEWG), operating under the 1st Committee of the UN General Assembly, deals with norms for state behaviour in cyberspace. 2. The new UN "Ad Hoc Committee" (AHC) has a mandate to draft a convention against cybercrime. 3. The Group of Governmental Experts for Lethal Autonomous Weapon Systems (GGE LAWS) is working on an agreement for drones and killerrobots. The author argues, that due to the complexity of the issues a reasonable involvement of non-state actors is needed to find workable solutions. The paper concludes, that conceptual disagreements about the future of the digital world between cybersuperpowers should not be an obstacle to selective agreement on stability in cyberspace.

Cybersecurity – Cybercrime – Robot Killer – Global Digital Compact

1. Introduction

On January 1, 2022, Germany assumed the presidency of the G7. Alongside climate change and the Corona crisis, cybersecurity is to be at the top of the agenda. That makes sense. The pandemic in particular has shown how dependent our world has become on a secure digital infrastructure. Instability in cyberspace is no less threatening to future generations than a destroyed environment.

Hardly anything has changed more in the last two decades than the Internet world. The Internet started as a promise of freedom and growth. Today it is seen more and more as a risk factor. Boundless communication and endless innovation have been overshadowed by the digital arms race, cyber espionage and blackmail software. On the Internet, everything seems to be pregnant with its opposite. Freedom and prosperity for some, Orwellian surveillance and exploitation for others. The Internet gives creative developers, innovative entrepreneurs and responsible citizens the same opportunities as hate preachers, pedophiles and warmongers. And it is still unclear who will gain the upper hand in this newly

W. Kleinwächter is a Professor Emeritus for Internet Policy and Regulation from the University of Aarhus. He was a member of the ICANN Board and a Commissioner in the Global Commission on Stability in Cyberspace. He is involved in Internet Governance issues since the early 1990s and has served in numerous committees in the UN, ITU, Council of Europe and the European Commission.

The paper is part of the Special issue "Internet governance and the challenges of digital transformation" edited by Laura Abba, Adriana Lazzaroni and Marina Pietrangelo.

flared-up struggle between "good" and "evil". If a "real war" were to break out today, U.S. President Joe Biden recently said, it would likely begin with a cyberattack.

In this respect, it is more than justified to make building a global cybersecurity architecture a priority for diplomacy in the digital age. The U.S. and China are heading toward a cold cyberwar. Digital attacks on critical infrastructure are proliferating. Internet-based drones, programmed with facial recognition software, seek out their own targets to kill. What can be done?

The good news is that governments and non-state actors have been talking about the risks and side effects of the information age for years. In 2005, a UN World Summit on the Information Society (WSIS) was held in Tunis. There, an "Agenda" was adopted with guidelines for a people-centered peaceful and open digital future. Since then, there has been the "Internet Governance Forum" (IGF), the UN's annual "digital summit." The next WSIS review conference is due in 2025. And other bodies have been formed under the UN umbrella to address cybersecurity, the digital economy and human rights in virtual space. So the world knows what dangers lurk in cyberspace and what should be done.

But the bad news is that virtually nothing concrete has been agreed so far. There is still a digital divide, regardless of all the progress of information infrastructure development in recent years with nearly five billion Internet users in 2022. There are massive violations of human rights in cyberspace with growing Internet censorship and mass surveillance. There are new oligopolies in the digital economy which hinder fair competition and innovation. Cross border data flow becomes part of a digital tradewar. And cyberattacks by state and non-state actors undermine global peace and international security.

20 years ago, WSIS was the only intergovernmental platform, dealing with Internet related public policy issues. Today there are numerous negotiations platform where governments and non-state actors from business, civil society and the technical community try to find solutions for the issues, which have emerged in the global Internet Governance Ecosystem since 2005, when the "Tunis Agenda" was adopted by 193 heads of state. UNESCO is dealing with artificial intelligence. ITU with the development of a digital infrastructure, WTO with digital trade, ILO with the consequences of digitalization for the labour market. The UN Human Rights Council is discussing how human rights, should be implemented in the online world. Based on the recommendations from a "High Level Panel on Digital Cooperation", chaired by Jack Ma from AliBaba and Melinda Gates from the Microsoft Foundation, UN Secretary General Antonio Guterres has published a "Roadmap on Digital Cooperation" in June 2020 and has now proposed a "Global Digital Compact" which could guide the world towards the 2030s.

However, all the negotiations didn't produce concrete arrangements with clear commitments. There are numerous reports and background papers on the various conference tables, but there is no agreement. There UN bodies – OEWG, AHC, LAWS – are negotiating security in cyberspace. But in all three groups, the controversies are greater than the will to agree on a common blueprint.

2. State behaviour in cyberspace

Lets have a deeper look into the global cybersecurity negotiations. Cybersecurity is now a core problem both of national and international security. And the numbers of attacks in cyberspace is growing.

The first negotiation platform is the Open Ended Working Group (OEWG). The OEWG was established in 2018 under the 1st Committee of the UN General Assembly. It was based on the work of several so-called "Group of Governmental Experts" (GGEs), which since 2004 worked on norms of state behaviour in cyberspace. The GGE could agree on eleven norms – including the norm not to attack critical infrastructures of other countries – and on a number of confidence building measures. It also agreed that international law and the Charter of the United Nations is relevant both offline and online. In 2020 the OEWG mandate was extended to 2025. All 193 UN member states participate in its work. Its task is to clarify what constitutes good behaviour by states in cyberspace in accordance with international law. Based on the agreement that international law applies not only to the analog world, but also to the digital world, this should not be a complicated task. There is no need to reinvent the wheel or to write a new UN Charter. But the controversies begin when things get concrete. When is a "cyber attack" a use of force that is contrary to international law under Article 2, paragraph 4 of the UN Charter and triggers the right to self-defense, laid down in Article 51? Is a "hack back" justified by Article 51 which constitutes the right to self-defence? Or can you asymmetrically answer a cyberattack with a bombing, which is what Israel did in Gaza after a cyberattack by Hamas? The problem is that not only there is disagreement about what exactly constitutes a cyberattack, but also the attacker is in many cases difficult to determine. If a tank rolls across the border, everyone knows where

it comes from. But if malware is installed in a power plant and is activated only after six months, it is not easy for the attacked state to prove one hundred percent where the attack came from.

Therefore, the OEWG is also about the role of non-state actors and confidence – and capacity – building measures. Ideas such as creating a permanent point of contact for crisis situations or organizing closer cooperation between technical experts and diplomats are reasonable steps. The first meeting of the OEWG in New York in early December 2021 took place in a thoroughly constructive atmosphere but it could not agree, how non-state actors will be involved in future negotiations. And it is also unclear what is actually supposed to come out of the negotiations: An action plan? A code of conduct? A cyber non-aggression pact?

3. Cybercrime

The second negotiation platform is about the exploding crime in cyberspace. For organized crime, virtual space has become more profitable than drug or human trafficking. There is already an international treaty against cybercrime: the Budapest Convention, signed in November 2001, just weeks after the terroristic attacks against the World Trade Center in New York on 9/11.

This treaty was drafted under the umbrella of the Council of Europe and it is open to every country for signature. Western countries have long campaigned to universalize the Budapest Convention, but only one-third of the 193 UN countries have signed it. Major Internet countries such as India, Brazil, and China were not involved in the negotiations and supported the Russian proposal to draft a new UN convention.

The concern of Western countries now is that new negotiations will undermine the regulations already in place and lower the quite effective standard of the Budapest Convention. Disputes are expected above all when it comes to the criminalization of information content. How are democracies and autocracies supposed to agree on what expression of opinion is permitted on the Internet?

The plan is that the new UN convention should be ready by the end of 2023. This is a tough timetable, but one that is nevertheless not entirely unrealistic. First, many passages of the Budapest Convention can easily be adopted. And second, the pressure of suffering generated by the global cyber mafia, with its extortion of hospitals and public administrations, and attacks on global supply chains and critical infrastructures, is now evenly distributed across ideological boundaries. If negotiators in the new Ad Hoc Committee (AHC) focus on what is feasible, progress would not be impossible.

4. Autonomous weapons systems

The third negotiation platform is about autonomous weapons systems. There, under the umbrella of the Convention on Conventional Weapons (CCW), a group of experts under the acronym LAWS (Lethal Autonomous Weapon Systems) has been negotiating killer robots and drones since 2014. UN Secretary General Antonio Guterres has been calling for a ban on autonomous weapons for years. But a very mixed group of states – Russia, China, the U.S., Israel, Turkey – have so far rejected even a moratorium. To be sure, there is fundamental agreement not to leave life-or-death decisions to an algorithm. But opinions differ even on the definition of what constitutes an autonomous weapons system. And while the filibustering continues in Geneva, the use of armed drones in local wars is becoming common practice, as in Nagorno-Karabakh, Yemen, Libya, the Middle East, in Ukraine and elsewhere. The problem is complicated. Maximum limits can be agreed upon for nuclear warheads, but what is the limit for an algorithm? Tanks and aircrafts can be counted and controlled, but how do you count and verify bits and bytes?

When it comes to autonomous weapons systems, the traditional rituals of disarmament negotiations are reaching their limits. More than ever, the political will of the actors involved and a minimum of trust are needed. And that depends in no small part on the extent to which it is recognized how a war with digital weapons could play out. NATO Secretary General Jens Stoltenberg recently recalled the time before World War One. Not only had the world "slipped into" a world war in 1914, he said, but the political leaders of the time had completely underestimated the effects of the new technologies of the time – from bombers and tanks to poison gas. Franz Haber, who later won the Nobel Prize for Chemistry and was involved in the development of chlorine gas in the early 1910s, convinced politicians that the use of this weapon would help bring about a quick end to the war. But he was wrong. The opposite was true. Millions of people died and chemical weapons became another source of instability in our fragile world. What would happen if Pandora's can of autonomous weapons systems were opened in a conflict today?

5. Technical Internet standards

And then there is a fourth negotiation platform: protecting the public core of the Internet. The functioning of the Internet infrastructure and the availability of the corresponding resources – root servers, domain names, IP addresses, Internet protocols – is now of the same elementary importance as water and electricity supplies. These resources are managed by various technical organizations – ICANN, IETF, RIRs. In 2016, after the US government – under the Obama administration – transferred its historic oversight of the Internet's A-root server to ICANN, there were repeated doubts, especially from China and Russia, about the ability of this technical community to manage technical resources in the interest of the global community.

But no disaster happened. On the contrary, if there had been a need for a stress test of the resilience of the system, which has been functioning for more than 20 years, the pandemic provided the proof. Since the Corona outbreak, there has been an exorbitant growth in Internet usage. Home office, zoom conferencing, online shopping, distance learning have all caused demand for domain names and IP addresses to explode. As it turned out, the existing system was able to handle these new challenges without any problems. There was no shortage of IP addresses or domain names. The root and name servers worked.

If these technical resources were to be drawn into a geo-strategic power play, there would be significant risks involved. Just as there is no Chinese or American air, only clean or polluted air, the technical Internet resources are politically neutral. If they became the plaything of a political arm-twist, everyone would suffer the damage. It was therefore very sensible that under the British G7 presidency the digital ministers clearly committed themselves to leaving the elaboration of technical digital standards in the hands of the technical community. The German G7 presidency should continue to pursue this path with vigor.

6. A dual strategy for cyberspace

The new German government in its role as chair of the G7 in 2022 is confronted with a broad range of challenges on the digital front. More than ever, the world needs a sustainable and fair multilateralism for cyberspace that is guided by the universal values of the United Nations Charter and the UN Declaration of Human Rights and embedded in close cooperation between governments, business, civil society and the technical community. With the G7 presidency, many eyes are now on Germany, which hosted the UN IGF in 2019. This also affects the negotiations on autonomous weapons systems. In January 2020, Green Party member of the Bundestag Katja Keul had criticized the then German government for not advocating strongly enough for a ban on these weapons under international law. The coalition agreement now states that the new federal government will take early initiatives on arms control in the areas of cyber and artificial intelligence. The German section of the non-governmental organization "Stop Killer Robots" has criticized this as far too soft. The EU has not yet positioned itself either. Katja Keul is now State Secretary in the German Foreign Office. This is an exciting task in which one can also learn from historical experience.

In early December 2021, the Friedrich Ebert Foundation held a conference to mark the 50th anniversary of the award of the Nobel Peace Prize to Willy Brandt. It wisely elaborated that Brandt's Ostpolitik was based on a dual strategy. The concept of "change through rapprochement" consisted both of an outstretched hand toward the system's rival and of strengthening the country's own resources. NATO's 1967 "Harmel Report," in which Brandt had participated as foreign minister of the then Grand Coalition, formed the basis for the creation of a web of "détente treaties" – from bilateral treaties between West Germany and the Soviet Union, Poland and the Czechoslovakia, via the Berlin Agreement (1971), the Soviet-US-SALT Agreements to the Helsinki Final Act (1975) – that ensured peace, at least for Europe, for several decades. The treaties of the 1970s were not based on the fact that the other social system was considered to be good. Here, people agreed to disagree. But there was an overriding interest in renouncing violence and protecting the common heritage of mankind that included the legitimate interests of the other side. Security was understood as collective security with the system rival, not against it.

Joseph Nye, doyen of American political science, reminded us in an essay "The End of Cyber-Anarchy", in the January 2022 issue of "Foreign Affairs", that in the Cold War temporary escalations of crises and stabilizing treaty negotiations were two sides of the same coin. Conceptual disagreements about the future of the digital world should not be an obstacle to selective agreement on stability in cyberspace. Wolfgang Ischinger, ex-head of the Munich Security Conference, also sees a reactivation of the principles of the 1975 CSCE Final Act and of the 1992 Charter of Paris as a sensible strategy to counter the new threats of the 2020s.

UN Secretary-General Antonio Guterres' proposal to use the UN Future Summit, scheduled for

2023, to adopt a "Global Digital Compact" could become an important building block for a new cybersecurity architecture. The idea floated by Finnish President Sauli Niinistö of using the 50th anniversary of the Helsinki Final Act in 2025 to promote security in cyberspace could be a good new beginning. In any case, if somebody will find the code for a lasting cyberpeace, she or he would be a good candidate fort the next Nobel Peace Prize.

* * *

Cercansi vincitori di Premio Nobel per la pace che creino la pace nel cyberspazio

Riassunto: Il saggio inizia con l'affermazione che per il futuro dell'umanità la sicurezza cibernetica è importante quanto la gestione del cambiamento climatico. Costruire un'architettura globale per la cybersecurity dovrebbe rappresentare una priorità per la diplomazia nell'era digitale. Il contributo tratta le tre principali piattaforme negoziali intergovernative sulla sicurezza informatica: 1. L'"Open Ended Working Group" (OEWG), che opera nell'ambito del Primo Comitato dell'Assemblea Generale delle Nazioni Unite, si occupa delle regole per il comportamento degli stati nel cyberspazio. 2. Il nuovo "Ad Hoc Committee" (AHC) delle Nazioni Unite che ha il mandato di redigere una convenzione contro la criminalità informatica. 3. Il "Group of Governmental Experts for Lethal Autonomous Weapon Systems" (GGE LAWS) che sta lavorando alla stesura di un accordo per droni e robot killer. L'autore sostiene che, a causa della complessità delle questioni, è necessario un ragionevole coinvolgimento di attori non statali al fine di trovare soluzioni praticabili. Il contributo si conclude sostenendo che i disaccordi concettuali sul futuro del mondo digitale tra le cyber superpotenze non dovrebbero costituire un ostacolo ad un accordo selettivo sulla stabilità nel cyberspazio.

Parole chiave: Sicurezza informatica – Criminalità informatica – Robot killer – Global Digital Compact