December 2019
#KASTalksTech

KONRAD ADENAUER STIFTUNG

The Road Towards Cyber-Sovereignty Passes Through Africa

Eleonore Pauwels

On November 18, UN Member States voted on a resolution led by Russia and China, paving the way towards a new global cybercrime treaty. The United States and its Western allies lost an opportunity to convince a majority of emerging and developing tech powers that multilateral, responsible governance can help them compete, boost, and build capacity for deploying converging cyber- and artificial intelligence (AI) technologies.

As developing countries line up behind China and Russia, the resulting normative alliance heralds the dawn of a new global order. Geopolitical dynamics will be shaped by multipolar competition over who, in cyberspace, owns and controls access to technological convergence – its intangible assets (datasets, source codes and tacit knowledge) and techniques, from AI, 5G, biotechnologies, to quantum computing.

As cybercrime continues to rise, increasingly targeting critical infrastructure of high and low-income countries, a new form of geostrategic competition centers around imposing national Internet surveillance and control.

Which governance model will ultimately prevail? The Sino-Russian model of cyber sovereignty and broad legal and normative definitions of cybercrime, or the Western model of shared, responsible governance and multilateral collaboration to close the global cyber-enforcement gap? Only time will tell, but the former is quickly gaining support from developing nations.

Cyber-sovereignty and China's Bridge to Africa

On November 18, fast emerging technological powers – including, Singapore, India, Kenya and South Africa – voted "yes" to support China's and Russia's normative effort. The UN cybercrime resolution passed 88-58 with 34 abstentions and 12 no votes. This vote brings the UN closer towards establishing a group of experts to draft terms of reference to define the scope of a treaty to counter the use of ICT for criminal purposes.

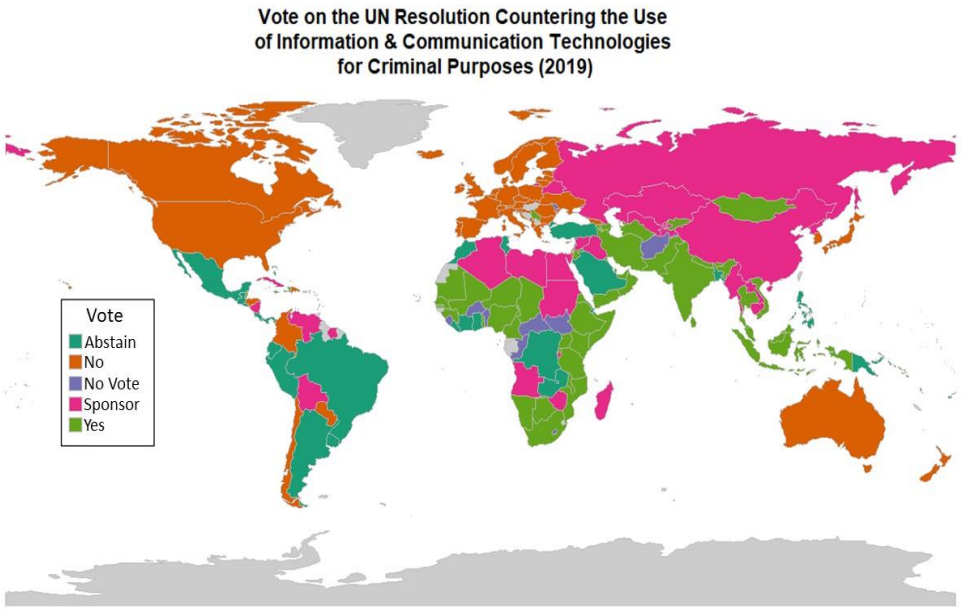
The proposed treaty is presented as a more global and inclusive alternative to the US-led Budapest Convention, which, ratified in 2011, aimed to support nascent forms of international cooperation, including transborder data-flows, to counter cybercrime and close the cyber-enforcement gap. Yet, the Budapest Convention was never endorsed by Russia and China.

Being able to access data and evidence across borders remains a critical step in cybercrime investigations and prosecutions. Yet, from Russia's and China's perspectives, the Budapest Convention raises important national sovereignty concerns over transborder access to information and electronic evidence. In particular, Article 32(b) permits states to obtain information in another country, without needing this country's government approval, if the lawful owner of the data gives consent.

From the Western perspective, at the heart of this new cybercrime resolution is an effort to establish UN-approved global norms that endorse national sovereignty over cyberspace. Such a move could duplicate, dilute, and hamper existing UN initiatives and international collaborations that already support global cyber-enforcement. A gradual balkanisation of cyberspace could even provide criminals with safe-havens from where to perpetrate cybercrimes with more impunity.

Not only that, but the normative vision proposed by Russia and China – which strategically omits to define "cybercrime" – could also be used to impose state control of the Internet, criminalise legitimate forms of online expression and uses of secure digital communications, as well as justify surveillance and repression of civil society in authoritarian countries. "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world," as stressed by the 2019 report of the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association.

While I share the concerns voiced by U.S. and European Officials and a long list of human rights groups, I am not taken by surprise. The evolution of geopolitics (below, map 1) – where China's Belt and Road Initiative builds new technological bridges to Africa and South Asia– reveals the changing power structures of cyberspace. We just need to examine and compare maps with acuity and foresight.



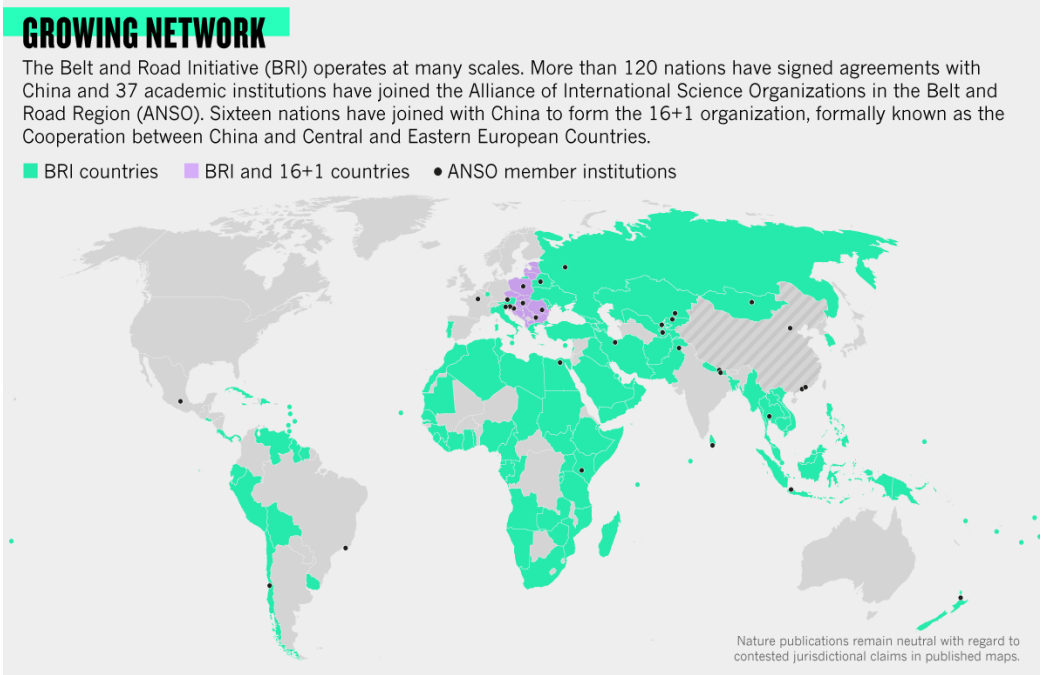
Source: Map based on 2019 Vote on Countering the Use of Information and Communication Technologies for Criminal Purposes (created by G. Dunlap, S. Denton and E. Pauwels.

Perhaps the most interesting aspect of the recent voting pattern is that the countries that either sponsored or voted "yes" to the cybercrime resolution also neatly overlays onto another map (below, map 2), the one redrawn by China under its Belt and Road Initiative.

This second map covers large parts of Africa and the South Asia-Pacific region up to countries in Latin America – showing the ever-extensive networks of more than 120 nations that are now partners in the Belt and Road Initiative (BRI). Among those states, a vast majority of African countries have already signed BRI scientific development agreements, from AI and satellite imagery projects to genomics agriculture. On the digital tech front, China is unmatched in Africa, with 5G and AI companies that are capturing more and more markets, to secure access to the 2 billion users that will rely on the next generation of the Internet.

What is at stake, beyond scientific collaborations, is a systematic long-term engagement by a tech-leading power to build and control the digital roads and bridges of cyberspace.

In addition to covering strategic military hotspots, the growing BRI network includes numerous large biodiversity reserves and targets countries that have access to the rare earth materials needed to power our digital and material revolution. For China, the long game is to acquire a global edge, to become a powerhouse in technological convergence, from AI, 5G and cybersecurity to biotechnologies.



Source : Masood E., How China is Redrawing the Map of World Science, Nature, May 1, 2019
https://www.nature.com/immersive/d41586-019-01124-7/index.html

China excels at the game of capturing markets, new materials, and massive data sets. Controlling the data (from consumption to bio-data) that will fuel artificial intelligence and genomics research translates into significant economic and security assets. Whoever gains a monopoly of these powerful resources may well be able to influence the well-being of entire populations and impact innovation in allied countries.

The Normative Language of Information Warfare

Cyberspace has become not only a new domain of fierce competition over information, business, and strategic technological operations, but also a new battlefield for projecting or undermining normative influence.

The near-future will see the rise of information warfare, more precisely what experts call "cognitive-emotional conflicts:" long-term, tech-driven propaganda aimed at generating political and social disruptions, influencing perceptions, and spreading deception. The centre

of gravity for at least some conflicts, such as Russia's intervention in Crimea or the Islamic State (IS)'s weaponization of social media, is shifting away from exclusive use of military forces towards targeting critical cyber and physical civilian infrastructures, political processes, and social cohesion of populations. The resilience of a nation and its political institutions ultimately lies in the minds of its citizens, who today are under constant pressure.

During the same month the UN General Assembly voted on the Russia-China led cybercrime resolution, the Russian government passed a 'sovereign Internet' law, which allows it to shut down Internet traffic from outside Russia in the context of 'emergencies' and to compel Internet service providers to use software that can filter and reroute traffic. Using computational, diplomatic and legal tools, Russia is carving up cyberspace into its own national cyber-domain.

This national effort aligns with the Russian sponsored UN resolution on a global cybercrime treaty, and its distinct lack of a definition of what cybercrime is and how digital technologies can be misused for criminal purposes. Such strategic omission creates legal uncertainty that can be harnessed to bypass international human rights law and criminalize the online behaviours of civil society, media, public, and corporate actors.

For Russia and other like-minded countries, the aim is partially, at very least, to carve up enough state control to develop and experiment with cyber-AI dual-use technologies that are strategic when waging information warfare, election-shaping operations, and cognitive-emotional conflicts.

Precision Surveillance Beyond Borders

By influencing global norms and technical standards, China's diplomatic efforts at the UN also aim to defend a form of cyber-nationalism that normalizes pervasive digital surveillance and new forms of political and social control. Personal, behavioural, medical, financial, and consumption data of about 20 to 30 million Chinese citizens have now been captured and aggregated to create digital profiles and rankings.

As shown on the Belt and Road map (Map 2), Beijing seems to be exporting its model of cyber-biopower to other nations, particularly developing and emerging economies in Africa and South-East Asia. For example, Thailand and Vietnam have adopted a similar approach to the Great Firewall – relying on a combination of legislative and technological tools to regulate the internet domestically. In the wake, Zimbabwe, Kenya, Uganda and Zambia have imported China's surveillance technologies.

The consequences of these approaches to precision surveillance could be corrosive. The entire history of individuals, populations, and professions could be leveraged – in intimate granularity, from online behaviours, dating patterns, and political preferences to medical records and drug consumption – for intimidation and discrimination. Combined with biometrics, algorithmic surveillance amplifies capacities for order and control, potentially leading to violations of human rights, freedom of expression, individual privacy, and agency. Even the perception of surveillance is enough to keep many in line.

AI-led Cybercrime and the Cyber-Enforcement Gap

The United States and its Western allies are concerned that the Russia-China-led UN resolution is about usurping control and governance of cyberspace, not building capacity to counter cybercrime. Entrenching national segmentations of cyberspace could even create new sanctuaries to launch far-reaching cybercrime activities.

One hard truth is that cybercrime is on the rise, amplified by the powerful combination of AI and cybersecurity, challenging law enforcement authorities in multiple jurisdictions. In March of this year, cybercriminals used speech synthesis to impersonate a CEO and order a transfer of about half a million dollars. In 2018 and 2019, Baltimore and Atlanta were paralyzed for

days under ransomware attacks, shutting down critical services such as airports and 911 emergency call centers. In Johannesburg and Hyderabad, ransomware attacks affected electricity companies' ability to respond to power failures. As early as 2016, cybercriminals hacked Bangladesh's Central Bank, stealing USD 81 million.

Increasingly, precision cyberattacks target biometrics data. In 2016, hackers stole the personal data of over 200,000 Malaysian organ donors and their next of kin to create fraudulent identities. In 2018, the Indian government biometrics database, Aadhaar, was the target of multiple cyberattacks that potentially compromised the ID profiles of large swaths of the 1.1 billion registered citizens. The Chandigarh-based Tribune newspaper reported that cybercriminals were monetizing access to the Aadhaar database at a rate of 500 rupees for 10 minutes. Elsewhere in the world in 2018, cybertheft of personal data impacted about 150 million users of the MyFitnessPal application, and around 50 million Facebook users.

As AI and cyber capabilities expand in developing countries, so too will the attack surface.

Deep learning will automate the identification of weaknesses in networked infrastructures. Automated cyber-operations will be more effective, finely targeted, difficult to attribute, and likely to exploit evolving vulnerabilities in AI systems. The capacity of adversarial algorithms to improve their own strategies and launch increasingly aggressive counterattacks with each iteration will lead to an expansion and augmentation of existing cyberattacks, with global damages that may reach USD 6 trillion a year by 2021. Yet, by 2023, the value of AI for cybersecurity is only projected to increase USD 17 billion.

A second hard truth is that countries with the greatest monetary losses from cybercrimes are the ones in the process of becoming digitized, but are still struggling to compete, build, and secure capacity in the development and deployment of AI and cybersecurity. As they fall victim to adversarial cyberattacks, they could become fertile operating grounds for cyber mercenaries, terrorist groups and other actors, increasingly compromising data-integrity and the robustness of

the globalized intelligence system. Many vulnerable States may not have the power, influence, foresight, or incentive to shape responsible governance of converging technologies towards social benefits and away from political disruptions and weaponization.

Technically, operationally, and legally, an array of governments across the globe are unprepared to close the cyber-enforcement gap. Cybercrime investigations often involve complex cross-sector and cross-border collaborations, which are difficult to navigate for some of the more powerful developed nations, let along emerging economies.

Cybercrime impacts low- and high-income countries differently depending on their cybersecurity capacity. While higher income countries such as the UK may have more security resources at their disposal, other countries like Malaysia are not as well equipped to handle large-scale cybersecurity breaches, such as the personal data leak of hundreds of thousands of organ donors, as noted above. Keeping pace with rapidly changing security threats will become increasingly more difficult, regardless of the country. Yet it will be the most vulnerable countries, the vulnerable links that will be impacted the most.

In this context of high vulnerability, for many countries struggling to secure their own cyber infrastructure, the Russian and Chinese cyber-sovereignty model may provide an illusion of proactive, tactical methods to manage cybersecurity threats and widespread disinformation campaigns, while offering new means to censor internal large-scale demonstrations. Over the past years, Internet shutdowns have become more frequent – with 134 instances in India during 2018 alone.

The Way Forward? Cyber-AI Prevention

Existing and future cybersecurity inequalities, not only in capacity-building but in prevention, will be significant in determining who flourishes and who fails in the converging technological future. At the same time, a complex understanding of converging risks does not underpin global development strategies.

Whose duty is it to foresee the unintended consequences of Cyber-AI convergence, and who possesses the required expertise for preventing harm? To meet these challenges, we need a common understanding of emerging security risks across the international community, driven by incentives for a shared approach to prevention.

I call it Cyber-AI Prevention: the urgent necessity and opportunity to tailor and adapt prevention capacities to the era of Cyber-AI convergence. Without prevention, the multilateral system will keep struggling to integrate AI and cybersecurity capacity-building into innovative global development strategies.

Last week in Berlin, the Internet Governance Forum offered a unique platform for dialogue between the worlds of diplomacy and the broader Internet community, including tech-leading companies and civil society actors. Similar conversations are taking place this week in New York under the auspices of the Open-Ended Working Group.

For those whose voices will be heard, I offer some advice to seize the opportunity: urge the private and civil sectors to collaborate with policymakers and multilateral organizations to translate the values of the UN Charter into norms, standards, and policies that promote responsible innovation in cyberspace. The cyber-insurance industry could become a partner in prevention in the AI-cyber era – not only prevention of AI-led cybercrime, but of other converging risks and social externalities. Only then will we be able to achieve Cyber-AI prevention.

Though the goal is ambitious, it is the only way to shape technological convergence so that it empowers vulnerable populations, protects human rights, and meets the ethical needs of a digitalizing and globalizing world.

Eleonore Pauwels is a Senior Fellow with the Global Center on Cooperative Security. Eleonore conducts in-depth research on the security and governance implications generated by the convergence of artificial intelligence with other dual-use technologies, including cybersecurity, genomics and genome-editing. Eleonore provides expertise to the World Bank and the United Nations, as well as to governments and private sector actors, on AI-Cyber Prevention, the changing nature of conflict, foresight and global security. In 2018 and 2019, Eleonore served as Research Fellow on Emerging Cybertechnologies for the United Nations University's Centre for Policy Research. At the Woodrow Wilson International Center for Scholars, she spent ten years within the Science and Technology Innovation Program, leading the Anticipatory Intelligence Lab. She is a former official of the European Commission's Directorate on Science, Economy and Society.

Eleonore regularly testifies before U.S. and European authorities including the U.S. Department of State, NAS, NIH, NCI, FDA, the National Intelligence Council, the European Commission and the UN. She is the author of a landmark report for the United Nations University, titled "The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI." Eleonore writes for Nature, The New York Times, The Guardian, Scientific American, Le Monde, Slate, UN News, The UN Chronicle and The World Economic Forum.

Konrad-Adenauer-Stiftung e. V.

Andrea Ostheimer
Executive Director
New York Office
www.kas.de/newyork

andrea.ostheimer@kas.de

The text of this publication is published under a Creative Commons license: "Creative Commons Attribution- Share Alike 4.0 international" (CC BY-SA 4.0), https://creativecommons.org/licenses/by-sa/4.0/legalcode