Cybernorms: Do They Matter IRL (In Real Life)?

Event report

RESEARCH ICT AFRICA

APC

GLOBAL PARTNERS DIGITAL

THE CENTRE FOR internet & society

Cybernorms: Do They Matter IRL (In Real Life)?

Event report

Veronica Ferrari (Association for Progressive Communications -APC), Sheetal Kumar (Global Partners Digital), Enrico Calandro (Research ICT Africa), Arindrajit Basu (the Centre for Internet and Society)

Introduction

The year 2021 saw several cyber attacks on critical infrastructure such as oil pipelines,[1] businesses such as airlines[2] and meat-packing companies,[3] and, crucially, healthcare providers such as vaccine suppliers.[4] Several of these attacks were attributed to nation-states while others were carried out by non-state actors. During the first half of the year, multilateral forums including the United Nations made some progress in identifying norms, rules, and principles to guide responsible state behaviour in cyberspace,[5] even though the need for political compromise between opposing geopolitical blocs stymied progress to a certain extent.[6]

There is certainly a need to formulate more concrete rules and norms. However, at the same time, the international community must assess the extent to which existing norms are being implemented by states and non-state actors alike. Applying agreed norms to 'real life' throws up challenges of interpretation and enforcement, to which the only long-term solution remains regular dialogue and exchange both between states and other stakeholders.

---

[1] William Turton and Kartikay Mehrota, "Hackers Breached Colonial Pipeline Using Compromised Password", *Bloomberg News*, June 5, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[2] Avlaw Aviation Consulting, "Cyber Attacks in the Aviation Industry", *Avlaw*, March 10, 2020, https://avlaw.com.au/cyberattacks-aviation-industry/.

[3] Julie Creswell, Nicole Perlroth, and Noam Scheiber, "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business," *New York Times*, June 1, 2021, https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.

[4] Reuters Staff, "IBM Flags More Cyber Attacks on COVID Vaccine Infrastructure", *Reuters*, April 14, 2021, https://www.reuters.com/article/us-health-coronavirus-vaccines-cyber-idUSKBN2C12EU.

[5] The two parallel processes at the UN First Committee concluded this year. See United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in the Context of International Security*, A/76/135, May 28, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; United Nations General Assembly, *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Final Substantive Report*, A/AC.290/2021/CRP.2.

[6] Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace", *Carnegie Endowment for International Peace*, May 19, 2021, https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491.

This was the thinking behind the session titled *Cybernorms: Do They Hold Up IRL (in Real Life)?* organised at RightsCon 2021 by four non-governmental organisations: the Association for Progressive Communications (APC), the Centre for Internet & Society (CIS), Global Partners Digital (GPD), and Research ICT Africa (RIA). Cyber norms do not work unless states and other actors call out violations of norms, actively observe and implement them, and hold each other accountable. As the organisers of the event, we devised hypothetical scenarios based on three real-life examples of large-scale incidents and engaged with discussants who sought to apply agreed cyber norms to them. We chose to create scenarios without referring to real states as we wanted the discussion to focus on the implementation and interpretation of norms rather than the specific political situation of each actor. Through this interactive exercise involving an array of expert stakeholders (including academics, civil society, the technical community, and governments) and communities from different regions, we sought to answer whether and how the application of cyber norms can mitigate harms, especially to vulnerable communities, and identify possible gaps in current normative frameworks. For each scenario, we aimed to diagnose whether cyber norms have been violated, and if so, what could and should be done, by identifying the next steps that can be taken by all the stakeholders present.

For each scenario, we highlight why we chose it, outline the main points of discussion, and articulate key takeaways for norm implementation and interpretation. We hope this exercise will feed into future conversations around both norm creation and enforcement by serving as a framework for guiding optimal norm enforcement.

Each scenario discussion was preceded by short scene-setting remarks by experts who had been invited to participate in the break-outs. These experts were Eneken Tikk, Moliehi Makumane, and Udbhav Tiwari (cyber espionage); Roxana Radu, Harriet Moynihan, and Rick Harris (critical infrastructure); and Justin Sherman (electoral interference). Following the short opening remarks, participants were invited to have an open discussion with the experts. In the summaries below, comments are not attributed to specific participants or experts.

Scenario 1 : Cyber espionage

Scenario 1

The intelligence agencies of State A conduct bulk surveillance abroad on government officials, citizens, and private actors. Through their private partners, the intelligence agencies are able to get access to data generated in multiple territories through various programs. One program uses a telecom provider to access high-capacity international fibre-optic cables, switches and routers throughout the world. Another uses data from the world's largest internet companies to access the content of communications abroad. There is no breach or attack—State A's surveillance dragnet relies on voluntary compliance.

In 2020, a hacker group allegedly affiliated with State B gained access to computer systems belonging to multiple government departments in State A. The attack involved the hackers compromising the infrastructure of LunarBreeze, a company that produces a network and applications monitoring platform. Subsequently, the hacker group used that access to produce and distribute trojanised updates.

The intelligence agencies of State A released a joint statement four weeks after the attack stating:

"This work indicates that an Advanced Persistent Threat (APT) actor, likely from State B is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence-gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly."

The Foreign Minister of State B responded with the following statement:

"We strongly object to and condemn State A's statement attributing the actions of a hacker group to us. They have not provided any credible evidence on record. In any case, this is merely an act of cyber espionage—-not forbidden in international law or emerging cyber norms discussions. State A's own extra-territorial actions are a case in point."

Why we chose the scenario

The Solar Winds attack is regarded by scholars as a "constitutive moment"[7] for international law on intelligence and espionage. Microsoft president Brad Smith has argued that "this is not espionage as usual…not just an attack on specific targets but on the trust and reliability of the world's critical infrastructure in order to advance one nation's intelligence agency."[8] Traditional

[7] Asaf Lubin, "Solar Winds as a Constitutive Moment: A New Agenda for the International Law of Intelligence," *Just Security*, December 23, 2020, https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.

[8] Brad Smith, "A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response," *Microsoft on the Issues,* Dec 17, 2020, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

scholarship posits that while international law does regulate espionage during war, there is no clear prohibition against peacetime espionage, which is left to the domain of domestic law. This position is being challenged of late. Buchan argues that both general principles of international law, such as sovereignty and non-intervention, along with specialised legal regimes, such as that of the World Trade Organization, apply to international espionage.[9] The volume, velocity, and variety of 'big data' generated as a result of bulk collection, as well as the scale of algorithmic filtering possible now, was unforeseen in the analogue age. However, these programs have largely been occluded at security forums and have instead been limited to human rights forums. A notable exception is the recent report of the United Nations Group of Governmental Experts (UN-GGE), which noted in their commentary on Norm 13 (e) that "State practices such as arbitrary or unlawful mass surveillance may have particularly negative impacts on the exercise and enjoyment of human rights, particularly the right to privacy."[10]

The scale and frequency of espionage-related cyber operations against businesses and government entities have increased. Further, extraterritorial mass surveillance continues to be accepted by the international community as an inevitability that is essential to safeguarding a state's 'national security' interests. Is there a legal or moral equivalence between offensive operations that result in industrial or political espionage and the passive monitoring of individuals' personal data without consent? The motivation for creating this scenario, loosely based on the Solar Winds attack and its aftermath, emerged from a desire to steer the cyber norms discussion towards meaningful regulation, and, where necessary, the outlawing of various practices that fall under the espionage umbrella.

Key questions for discussion and session summary

1. Does international law presently outlaw espionage? Therefore, is cyber espionage legal?
2. Has cyber espionage been adequately discussed at global forums? Is State B correct in saying that even if it engages in it, its actions should not attract censure?
3. Can the actions of State A's intelligence agencies be equated with the attack allegedly perpetrated by State B?

The session started with a discussion on whether espionage is legal under international law. Participants argued that while espionage is not 'illegal', the position would likely not hold up under full scrutiny, as it is not in line with the law governing peaceful international relations between states. The avoidance of meaningful global discussion has been rendered possible due to the 'skilful efforts' of a group of states who seek to avoid public scrutiny.

One expert outlined a few points to consider for states looking to build a case against cyber espionage. These include:

---

[9] Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing, 2018).
[10] United Nations General Assembly, *Report of the Group of Governmental Experts*, pp. 8 para 37.

a) Strong arguments can be built on espionage violating particular obligations under international law, notably territorial sovereignty, prohibition of intervention, international human rights, and diplomatic privileges.
b) States must consider whether protections to states and civilians during war must be extended during peacetime as well; they must also weigh how espionage impacts bilateral relations.
c) An international dialogue or an explicit inquiry into the status quo would reveal potential weaknesses in the prevailing view.
d) How can domestic laws be refined to better reflect the state's views?

With regard to the second point, participants posited that the debate is both complex and nuanced. States are using ICTs (information and communication technologies) to indulge in espionage activities while the market for cyber vulnerabilities is booming. Theft of intellectual property is another allied concern. Despite the absence of specific norms against espionage, there exist other norms such as the norm on resilient supply chains which have coercive value to prevent nation-states from incorporating 'backdoors' into critical infrastructure and equipment. An expert further pointed out the significance of norms on attribution and vulnerabilities disclosure. States should be provided adequate room to decide how and when a vulnerability should be disclosed depending on the trade-offs between the vulnerability being an important intelligence-gathering tool and an opportunity for a state or non-state adversary.

An expert also spoke of the specific role of vulnerability disclosure among nation-states as a key tool for confidence-building. Cooperation in the mapping and management of vulnerabilities is increasing, especially among stakeholders in the business community. Domestic frameworks are also emerging, such as norms that states can implement within their boundaries and jurisdictions. These laws need to emerge not unilaterally but through international dialogue. An example of such a law is the EU Cybersecurity Act.[11] One expert adduced a note of optimism, arguing that nation-states are beginning to understand the importance of establishing common cybersecurity standards, which is an encouraging sign.

The participants did not explicitly answer the question of fault (or in international law terms, 'responsibility') on the part of State A or State B. That was to be expected, given the complexity of the scenario and the fact that legal and normative frameworks are evolving dynamically. The most appropriate conclusion for the discussion on assigning blame, perhaps, in the words of an expert, is "*There is a lot of nuance with regard to who is wrong, if anyone is wrong, and maybe it shouldn't matter because it can put a full stop where we should have a pause in terms of engagement.*"

[11] "The EU Cybersecurity Act," https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

Key takeaways

- The traditional international law position that cyber espionage exists in a 'gray zone' and is not illegal requires consideration and re-evaluation, particularly in today's age of big data and surveillance.
- While there are no explicit norms countering espionage through technological means, norms on supply chain resilience and vulnerability disclosure are more practical and easily implementable avenues of getting to a broader norm on espionage
- There has been greater co-operation in the last few years between industrial players on vulnerability disclosure. There is scope yet for more co-operation between States to ensure that domestic law and policy is not made unilaterally but in consultation with external States and other stakeholders. Convergence between States and other stakeholders across regions should remain a priority.

Scenario 2 : Attack on critical infrastructure

Scenario 2

A major cyber attack occurred in May 2021. It targeted the SAAP cargo management port system, a ports information management system provided by a Northern European company, and compromised supply-chain operations of Suez, Djibouti, Kollam, Durban, and Dakar ports, severely affecting the global maritime supply chain. The interruption in the supply of essential services such as COVID-19 vaccines and basic necessities across Africa and India impacted humanitarian aid projects aimed at providing relief to countries in the Global South affected by the pandemic. Specifically, the attack impacted the operations of the WFP, FAO and COVAX programme.

A global coalition of European, African and Asian governments is working with INTERPOL, EUROPOL, and AFRIPOL to identify the attacker.

The attack, which compromised the tracking systems of the cargo at the harbours, has the potential to considerably delay the rollout of vaccines in many African countries and in India. Also, the supply chain of basic necessities has been compromised.

Why we chose the scenario

Since the 2003 United Nations General Assembly (UNGA) Resolution 58/199 on the "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures",[12] UN member states have increasingly recognised the links between countries' critical infrastructures and their critical information infrastructures, and the associated

[12] UN General Assembly, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures", resolution no. 58/199, https://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

transnational cyber risks. In addition, in UNGA Resolution 64/211, member states expressed concern regarding the growing sophistication of attacks and the gravity of damage to critical information infrastructures and to the integrity of the information and services. Through the adoption of UNGA Resolution 70/237 in 2015, member states welcomed the applicability of international law, in particular the UN Charter, to maintain peace and stability and promote an open, secure, stable, accessible, and peaceful ICT environment. They acknowledged that "the most harmful attacks using ICTs include those targeted against the critical infrastructure." Last but not least, the 2015 UN Group of Governmental Experts (GGE) set voluntary, non-binding norms, rules, or principles of responsible behaviour for states explicitly protecting critical infrastructure.

Key questions for discussion and summary of discussion by participants

During the session, the key experts and participants were asked to address the following questions:

- Were any existing cyber norms violated, and, if so, which ones?
- To what extent do existing norms mitigate real-life cyber incidents like attacks on critical infrastructures?
- Would an additional or different norm (or another policy or regulatory measure) have prevented/mitigated the attack?

The expert contributors agreed that it is important to distinguish between norms and obligations under international law. Establishing this distinction became even more critical after the COVID-19 outbreak. In that context, for instance, an international group of lawyers released a statement titled "The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector",[13] which emphasised that cyber operations do not occur in a normative void or a law-free zone. It recommended that rules and principles of international law should protect medical facilities against harmful cyber operations.

At the same time, discussants emphasised that both the development of international law and how it applies to cyberspace are taking time. This is because there is an interplay between different measures when it comes to the development of international law—e.g., the Tallinn Manual, state practice and national positions being shared, and case laws (there isn't much yet, but it is expected that there will be more). Therefore, even without a treaty, experts agree that we are witnessing greater concretisation of legislative measures in cyberspace. Viewed in this way, international law obligations already protect the integrity of supply chains, as well as GGE norms 13.i, 13, f., 13.g.

Norms, although voluntary and non-binding, provide recommendations that help states protect domestic critical infrastructure as well as expect specific behaviours against other states internationally. Norms and international law can also inform domestic law on critical infrastructure protection.

---

[13] "Oxford Statement on the International Law Protections against Cyber Operations," https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea#/

Similarly, other instruments, such as industry obligations, may require the implementation of security by design, although these instruments are not enough to avoid vulnerabilities in IT/network systems.

Nevertheless, it is well known that many cyber operations happen secretly 'behind the scenes', undermining the effectiveness of norms in mitigating harm. Norms are a form of soft law that is probably not enough. At the same time, norms help increase alliances between countries to identify criminal cyber actors as well as foster coalitions between the public and private sectors. Norms also relate to each other and to other elements of the GGE report. For instance, norm G on the global culture of cybersecurity is linked to cyber capacity-building. Therefore, they should not be assessed in a silo but in conjunction with other elements including IL. Some principles, such as due diligence, are already obligations under international law. Some states consider due diligence a binding principle, indicating that soft law might be materialising into hard law obligations— a sign that international cybersecurity governance is gathering momentum.

In the recently adopted GGE report, the adoption of new norms is discussed. However, existing norms are still being adopted slowly in some countries while others find it challenging to implement them. Countries also wait for 'something bad to happen' before they adopt them. Therefore, there is a need for broader adoption of existing norms. In the conclusions of the session, experts agreed that existing norms should not change, as that would bring about an entirely different approach to state behaviour in cyberspace. Nevertheless, they emphasised that more preparedness and resilience are required, primarily through capacity-building.

Key takeaways

- It is important to distinguish between norms and obligations under international law (IL). IL obligations protect the integrity of supply chains, as well as GGE norms 13.i, 13, f., 13.g.
- Norms have set expectations to behave in a specific way but there is a need to domesticate norms taking into account that different States have different challenges/ability to implement them;
- The development of IL and how it applies to cyberspace is a lengthy process, although different measures (at an international as well as at a national level) are leading towards more concretisation of legislation on cyberspace.

Scenario 3 : Electoral interference

Scenario 3

State A has a major election coming up. In the weeks prior to the election, a series of cyber-enabled incidents take place, all of which independent researchers later assert to be cyber operations of the intelligence service of State B. The incidents include:

- Publication of unverifiable information on specific candidates, particularly in media outlets known for the dissemination of so-called fake news and for promoting views close to those held by the regime in State B. Trolling discussions on candidates' profiles on social media platforms, with posts often made by user accounts that have either been recently established or cannot be verifiably linked to a real person.
- A large batch of private emails, purportedly exchanged only among members of one candidate's campaign team, is leaked onto a well-known, publicly accessible internet site.
- Advertisements compromising candidates' credibility are published in print and online media, while the entity who commissioned them is either clearly artificial or known to support these candidates' electoral opponents or the regime in State B.

Why we chose the scenario

We chose this scenario as electoral interference is identified in the GGE and Open-ended Working Group (OEWG) reports as a cyber threat, and there have been high-profile cases of electoral interference by states (i.e. Cambridge Analytica). However, while a number of countries have defined electoral infrastructure as critical infrastructure, it is not widely or universally defined as such. Furthermore, the question of whether electoral interference is a violation of sovereignty or when it is remains unclear. Yet this lack of clarity is a problem, as electoral interference is a threat to democracy and the right to free and fair elections.

Key questions for discussion and summary of discussion by participants

During the session, the key experts and participants were asked to address these questions:

- Were any existing cyber norms violated, and, if so, which ones? Did the operation interfere with human rights? If so, which rights were affected by this operation?
- Would an additional or different norm (or another policy or regulatory measure) have prevented/mitigated the attack?
- To what extent are existing norms mitigating real-life cyber incidents like electoral interference? How can norms do more?

The first issue that was highlighted by participants was that there is a definitional lack of clarity, since there is no agreed definition of what electoral interference is.

Participants also noted that this is a complex matter and there is no singular answer to the question of which existing cyber norms were violated. There is no strong/established norm against electoral interference. Though sovereignty and the principle of non-interference broadly relate to this topic, electoral interference remains difficult to pin down as there are many undefined aspects—e.g. does it refer only to attacking or infiltrating infrastructure or does the dissemination of information also count? For example, which targets count as attacks on electoral processes? Furthermore, normative frameworks are not binding and require reciprocity and mutual understanding.

Therefore, one option could be to more precisely define electoral infrastructure and develop norms against attacking that. Or norms could be developed with respect on the specific technical measures being used to then protect those different elements, like encryption, or security processes for protecting voter confidentiality. We should also keep in mind that other stakeholders can help shape understanding. For example, we could look at what social media platform policies define as acceptable/unacceptable information.

We need this to know when norms are violated, which is key, because norms without accountability do not serve any purpose. However, attribution remains a challenge. Greater cooperation among states is also required at the international level. At the same time, there is an urgent need to domesticate cyber norms by engaging policymakers at the national level to shape national public policy.

Regarding the need for additional or different norms (or other policy or regulatory measures), participants stressed the importance of implementing existing measures and norms and increasing accountability around this implementation.

Key takeaways

- Greater clarity on definitions is required (e.g more granular understanding of what electoral interference means/how it is understood)
- Norms are important but there are more than normative frameworks. There is a need for practical use of norms and, for this, domesticating norms at national level is essential.

Conclusions and next steps

With regard to substantive norms and law, definitional clarity is key. Member states should work with stakeholders to develop terms and definitions, including, for example, what type of actions constitute electoral interference and/or the technical measures used. For example, we could more precisely define electoral infrastructure and develop norms that protect it from being attacked. The challenge with cyber norms currently is that they are non-binding and do not create legal obligations. The pathway we could adopt, therefore, is enabling cooperation on the technical implementation of norms, which will pave the way towards establishing 'hard' norms. Discussions on the applicability of international law obligations may be a useful example here. While the jurisprudence of the International Court of Justice and international scholarship have weighed in on the obligation of due diligence, states have incorporated this principle differently when it comes to ensuring cyber hygiene to prevent non-state actors from using a state's territory or ICT infrastructure to carry out internationally wrongful acts. The UN-GGE's 2021 report concluded that due diligence is an 'expectation' and not an obligation when it comes to cyberspace. While this articulation may not be entirely accurate in terms of international law, it offers an opportunity to engage in wide consultations with states to come up with a narrow set of binding obligations that would form the content of 'international law of due diligence in cyberspace'.

In terms of creating a global institutional architecture, it is important to think outside the box and engage all relevant actors in implementing a norm—for example, when it comes to electoral interference, social media companies are developing and implementing policies aligned with relevant cyber norms. Additionally, with regard to vulnerability disclosure, industrial actors are taking the lead.

On implementation, independent attribution remains a key challenge, as does the need to nationalise implementation by engaging domestic stakeholders. Questions for future research might include how various interested stakeholders can come together for the purpose of collective attribution. Depoliticising discussions on cybersecurity and stability allow for vibrant discussions on specific legal or technical questions pertaining to norm implementation, as states take steps to internalise or implement emerging norms. All three scenarios fostered discussions on existing norms but simultaneously advanced questions regarding the extent to which each norm could adequately regulate or defuse tensions resulting from the scenario. Cyber norm formulation and implementation will always involve political processes and foreign policy posturing by states, and rightfully so! Our session merely demonstrated that addressing norms in real life (IRL) through the lens of hypothetical scenarios offers an opportunity for all stakeholders to critically appraise the extent to which a norm might play out in legally and technically complex scenarios.

We also intend to leverage this report within the framework of the UN First Committee's upcoming OEWG on ICTs.

Acknowledgements

We are very grateful to all the speakers and participants at the session, Anand Badola for facilitating and rapporteuring the session and to The Clean Copy and Lori Nordstrom, APC Language coordinator, for their edits on this draft. All errors remain our own.