The UN Cyber Norms:

How Do They Guide the Responsible Development and Use of Offensive Cyber Capabilities?

Bart Hogeveen

ABSTRACT

In this article, I review how the international cybersecurity norms, agreed to in 2015 and reaffirmed in 2021 by the member countries of the United Nations (UN), provide guidance to states on their possession and use of offensive cyber capabilities. This is an important exploration given that UN negotiations have reached a provisional climax, and that more states, ranging from major cyber powers to developing cyber nations, are getting involved with offensive cyber activities. I consider the 11 UN norms and extract the specific guidance they offer both to states that conduct offensive cyber operations and to states who have been attacked by offensive cyber activities. Then, I consider the various types of cyber operations that could affect international peace and security before looking at ways through which governments, international bodies and communities of non-governmental organizations can support observance of the UN norms. Finally, I assert that responsible forms of offensive cyber will not be for all states, and that raising the bar – including through the UN norms – benefits all major cyber powers.

At the informal intersessional consultative meeting of the UN Open-ended Working Group (OEWG) on information and communications technology (ICT) security in December 2019, Microsoft's vice-president for Customer Security and Trust, Tom Burt, wanted to send a strong message to the assembled representatives of UN member countries: the security, safety, and stability of cyberspace is in imminent danger and, to prevent further escalation, countries should stop misusing

Bart Hogeveen is the Head of Cyber Capacity Building at the Australian Strategic Policy Institute. In this role, he focuses on international peace and security, international aid, and national security aspects of cyber and digital issues in the Indo-Pacific region. Together with ASEAN-based think tank partners, he authored the Sydney Recommendations on Practical Futures on Cyber Confidence Building in the ASEAN region (2018). With support from the UK Foreign, Commonwealth and Development Office and the Australian Department of Foreign Affairs and Trade, Bart directed a multiyear capacity-building effort supporting the implementation of the UN cyber norms in the ASEAN region between 2019 and 2021. His report, "The UN norms of responsible state behaviour in cyberspace. Guidance on Implementation for Member States of ASEAN," was published in March 2022.

cyberspace for offensive operations.[1] In the accompanying written submission, Microsoft stated that it was analyzing "trillions of signals" in an effort to "identify sophisticated threats and protect our customers from a diverse and growing number of nation-state actors."[2]

In 2018, the UN General Assembly established this OEWG to further develop norms for states' responsible cyber behavior, explore ways to implement them, and, when necessary, introduce changes or additional rules of behavior.[3] After two years of negotiations, the working group concluded in 2021 with a reaffirmation of 11 voluntary and non-binding norms that were first agreed in 2015.

The 11 UN cyber norms set out eight positive steps that states should take, and three actions states should avoid.[4] States are recommended to implement the following actions:

- Cooperate to increase stability and security in cyberspace
- Consider all relevant information when attributing cyber incidents
- Prevent criminal and terrorist use of information and communications technologies
- Respect human rights—including privacy—online
- Take appropriate measures to protect critical infrastructure from cybersecurity threats
- Respond to reasonable requests for assistance from another state
- Take steps to protect the integrity of supply chains for ICT products, and
- Report ICT vulnerabilities in a responsible manner

And states should refrain from the following actions:

- Knowingly allow their territory to be used to commit internationally wrongful acts using cyber tools

- Conduct cyber activities that damage the delivery of essential services by critical infrastructure in another country
- Harm another country's Computer Emergency Response Team (CERT) or use their national CERT to engage in malicious cyber activity

Throughout the tenure of the OEWG negotiations, between 2019 and 2021, the message from industry, civil society organizations and thinktanks was that governments should act in a more diligent, forthcoming, and sincere way in complying with their self-agreed norms.[5] This is a challenge when compliance is based on political and moral grounds and detailed guidance, case-studies and verification methods are absent.

As more states (both major cyber powers as well as developing cyber nations) add offensive tools to their portfolio of cyber capabilities, so should the accountability and reassurance measures. Therefore, the main question that I intend to answer in this article is: How does the existing set of UN norms provide relevant guidance for states in their efforts to responsibly develop, possess, and deploy offensive cyber capabilities?

Competition and conflict among states and their use of cyber tools as levers of political, military, and economic coercion are generally regarded as threats that can potentially destabilize the integrity of cyberspace and societies that rely on trust and confidence in the digital environment.[6] Since 2015, the number of state-sponsored cyber operations and significant cyber incidents that have become publicly recorded or acknowledged has grown significantly (See figure 1).

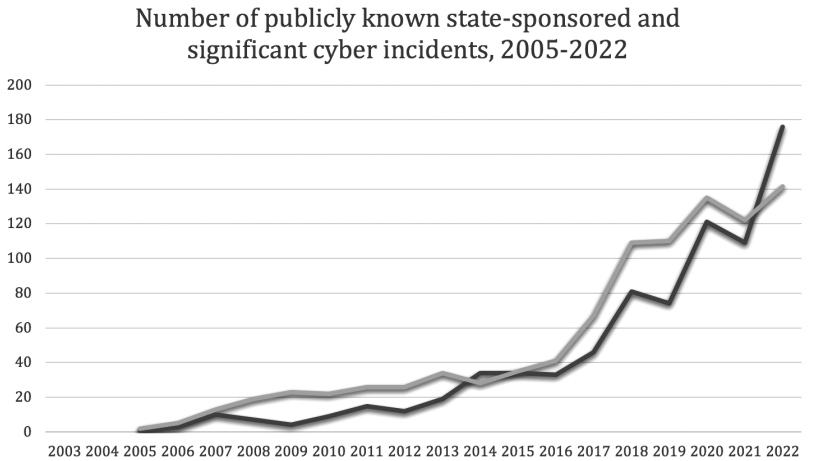

Figure 1. Based on number of entries per year from Council on Foreign Relations' Cyber Operations Tracker (black line) and the Centre for Strategic and International Studies' List of Significant Cyber Incidents (gray line).

Specifically, the governments of Russia, China, North Korea, and Iran have attracted the ire of western states for sponsoring offensive cyber operations. In July 2021, a grand coalition of the US, UK, Australia, Canada, New Zealand, Japan, the EU, and NATO called out the Chinese government for a prolonged campaign of espionage that sought commercial and personal profit,[7]

discovered and exploited zero-day vulnerabilities in Microsoft Exchange servers[8] and aided "the widespread and reckless sharing of the vulnerability."[9]

The public statements accompanying the attribution refer to internationally agreed norms of responsible state behavior.[10] In this case, among other things, China was called upon to honor its commitment not to "knowingly allowing its territory to be used for internationally wrongful acts using ICTs" (UN norm #3). After being notified, China should have taken "reasonable steps within its capacity to end the on-going activity in its territory," which it declined. Moreover, should Beijing lack the capacity to address these issues, norm #8 suggests it should have considered seeking outside assistance, which it did not.

There are, however, commitments that the attributing states had to uphold as well. UN norm #2, for instance, recommends that states "consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences."[11] They should also keep in mind that "an ICT incident emanating from the territory or the infrastructure of a third state does not, of itself, imply responsibility of that state for the incident."[12]

Overall, the practice of publicly attributing acts of offensive cyber appears a bit one-sided. All documented attributions have originated from western governments, dominated by Five Eyes nations, which have declared their own possession of offensive cyber capabilities and a willingness to use them. In fact, the US, UK, Australia, as well as the Netherlands, Denmark, and Sweden have confirmed they have conducted offensive operations.[13]

Despite ample public evidence to the contrary,[14] officials representing the governments of China, Russia, and Iran have continued to deny their country's possession, and use of offensive cyber capabilities.[15] In international forums, Beijing, Moscow, and Tehran have gone to great lengths to object to any language that would normalize what they call the militarization of cyberspace.[16] They capitalize on sentiments expressed by developing cyber nations, such as through the Non-Aligned Movement, which feel overwhelmed by the capabilities of major cyber powers.[17]

This case illustrates how the UN norms can be used to guide state practice. There are certain rules, principles, or norms—either explicit or implied—that determine a 'zone of acceptable behaviour' when it comes to the possession and use of offensive cyber capabilities and any state's (counter)responses. At the same time, today ample latitude remains for states to deny or circumvent their responsibilities and dodge accountability.

Are the 2015 UN Norms Relevant for the Future of Offensive Cyber?

Efforts to build an international regime for managing inter-state cybersecurity issues started as early as 1998. One of the milestones has been the endorsement by the UN General Assembly of Resolution 70/237 in 2015, which calls on all states to use the UN framework for responsible state behavior. This framework is based on the recognition that international law applies to state

behavior in the cyber domain and is further complemented by 11 voluntary and non-binding norms; various confidence-building measures, particularly to strengthen transparency, predictability, and stability, and; a commitment to global capacity building.[18]

The set of 11 norms probably provides the most practical guidance regarding what is expected of states in their use of ICTs.

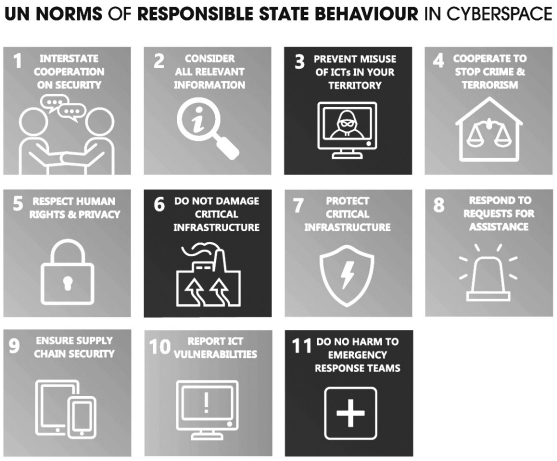

Figure 2 The UN norms of responsible state behaviour in cyberspace. Source: https://www.aspi.org.au/cybernorms.

Since 2015, three more rounds of negotiation have taken place. A setback was encountered when the Group of Governmental Experts (GGE) 2016-17 failed to reach a consensus. Disagreements remained over the application of international law, the right to self-defense, the principle of state responsibility, and legal bases for countermeasures in response to a cyber incident.[19] The latest two rounds, the Open-ended Working Group and sixth GGE which occurred in parallel in 2019-21, were successfully concluded. This reestablishment of consensus among the OEWG and GGE members has been hailed as a diplomatic triumph.[20]

Negotiators were able to add references to cybersecurity threats affecting electoral processes and health infrastructure,[21] and to rebut claims that "the consensus of the past is not the consensus of the present."[22] Besides this, however, the national delegations were only able to agree to a reconfirmation of the previous agreement from 2015. Therefore, it is reasonable to assume that negotiations have now reached their provisional climax, and the reach and breadth of the framework will not be expanded in the near future.

At this point in time, the UN framework of responsible state behavior in cyberspace is the only globally recognized point of reference to assess what is and what is not responsible state use of cyber tools in the context of international peace and security. Hence, negotiators have shifted their attention to deepening their understanding of the practical implications of the current framework, in particular the norms.[23] These could include guidance on responsible use of offensive cyber capabilities, requirements for oversight and accountability, and recommended

operational policies, skills and safeguards a state should be able to demonstrably possess—now and into the future. There may also be certain monitoring and reporting roles that could be taken up by academia, civil society organizations, and industry to increase transparency, accountability, and strengthen collective reassurance.

For this article, offensive cyber capabilities refer to a state "possessing the resources, skills, knowledge, operational concepts and procedures" to conduct offensive cyber operations which are "operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks."[24] As I am focusing on international peace and security, I consider a cross-jurisdictional element as a factor in offensive cyber operations.

There is no implied suggestion that states should develop offensive cyber capabilities or consider their use, let alone that this would be a positive development for international peace and security. However, it is taken as a matter of fact that states are increasingly working on developing sophisticated offensive cyber capabilities and that more states, for different reasons, will get involved with offensive cyber capabilities in the future.

Can the Future of Offensive Cyber be Assessed through the UN Norms?

With the agreed upon UN cyber norms, the activities, intentions, and policies of states can be subjected to assessments.[25] States can be complimented for their response to an incident, or national practices can be heralded as global good practice. Also, states can be reprimanded if they have not done enough to prevent an incident, or that they have used cyber capabilities in an irresponsible manner.[26]

The language reflected in the current text of the norms is a result of concerns and opinions following cyber and information security incidents that occurred up to 2015 such as the 1999 wars in Kosovo and Chechnya,[27] the Olympic Games/Stuxnet[28] operation against Iran, and the Snowden revelations.[29] Since then, there have been attempts to introduce additional norms, notably the idea of protecting the "core of the internet" (promoted by the Netherlands), to prohibit cyber-enabled theft of intellectual property for commercial purposes (promoted by the US) and including the application of international humanitarian law (IHL); spearheaded by the International Committee of the Red Cross (ICRC). Although the GGE in 2021 agreed to note that IHL applies as well as the applicability of its underpinning legal principles,[30] neither the GGE 2016-17 nor the two 2019-21 groups succeeded to expand the original 11 norms.

There have also been proposals from civil society organizations and the IT industry to expand the remit of the UN norms and make them apply to issues of digital rights, cybercrime, and digital development. However, UN member states have rebuked this sentiment and maintain that the norms should focus on cybersecurity issues *that affect inter-state relations*.[31] While recognizing the multi-stakeholder nature of the cyber domain, in particular ownership of key tenets of infrastructure by the private sector, governments also held on to their primary responsibility to ensure safety and security in inter-state cyber relations.[32]

The norms are seen as a means for states to prevent and mitigate the worst of all cyber incidents, i.e., those intentionally or inadvertently perpetrated by governments in the context of political-military tensions or economic conflicts. Offensive cyber falls squarely within this context. Additionally, the UN norms serve as a foundational source from where to deduce specific guidance on responsible state use of ICTs and should be used to assess current state behavior and draw red lines for future reference. In fact, the 2021 reports of both the OEWG and GGE introduced a line calling on states "to avoid and refrain from the use of ICTs not in line with the norms of responsible State behaviour."[33]

How do the UN Norms Examine Offensive Cyber?

The UN working groups that were established to consider international cybersecurity were, among other things, instructed to provide an assessment of existing, emerging, and potential threats. Since 2004, none of the reports that have been published makes explicit reference to offensive use of cyber capabilities.[34] Instead, UN member countries simply acknowledge that "a number of States are developing capabilities for military purposes"[35] and observe activities by "persistent threat actors, including states" as well as the use by states of "ICT-enabled covert information campaigns."[36]

These rather unspecified acknowledgments reflect observations that cyber operations tend to be mostly conducted in "the grey zone," which characterizes many of today's conflicts, tensions and strategic competition.[37] Within this zone, we see blurred lines between intelligence and offensive cyber operations; between cyber and information operations; in the use of proxies for cyber operations; and the absence of a distinction between operations of a criminal or inter-state (political-military, offensive) nature.

The UN norms, however, do refer to certain cyber capabilities that states possess and use that are potentially of an offensive nature. These terms are laid out in Table 1.

Table 1: Terms related to offensive cyber included in the UN norms lexicon.

Norm	Terminology
#1	ICTs, ICT networks, and ICT practices that are harmful or that may pose threats to the maintenance of international peace and security
#2	Malicious ICT incidents
#3	Internationally wrongful act
#6	ICT activity contrary to obligations under international law
#6	ICT activities conducted or supported by a state that may impact the critical infrastructure of or the delivery of essential public services in another state
#8	Malicious ICT acts
#9	Malicious ICT tools and techniques
#9	Use of harmful hidden functions, including backdoors
#10	The exploitation of vulnerabilities that compromise the confidentiality, integrity, and availability of systems and networks
#11	Malicious international activities

The used terminology suggests that the international community intends to distinguish between the malicious and benevolent use of cyber capabilities. This may imply that offensive cyber operations are acknowledged in situations where acts, tools, techniques, and activities are or are becoming "malicious." This leads to questions about what is considered "malicious" and who makes that determination.

The potential consequences of offensive use of cyber capabilities seem to be recognized with the adjective clauses "acknowledged to be harmful" and "pose a threat to international peace and security." Finally, the terms note the use of hidden functions in software and/or the exploitation of known or yet unknown vulnerabilities. These are tools, tactics, and techniques—or enablers—that commonly form a part of offensive cyber operations. Clearly, the UN norms do not dismiss the existence of a state's offensive cyber repertoire although precise definitions and intended meanings are absent.

What Guidance Can be Deduced from the UN Norms on Offensive Cyber?

A next step is to look closely at the text of each of the individual norms and establish how they address the pertinent issues such as the development of offensive cyber capabilities, command and control over cyber tools in possession; use of cyber capabilities; and response measures after becoming a victim of the development, control, and/or use of capabilities by other states. This is greatly aided by the "additional layer of understanding"[38] that is offered in the GGE 2021 report.

An initial observation in considering the eleven norms is the balance between responsibilities of the victim of a cyber operation and those of the author. This is most evident in the combination of norms 6 and 7. While norm 6 prohibits the targeting of critical infrastructure in another state, norm 7 imposes a responsibility to make sure one's own critical infrastructure is sufficiently cyber secure. This should create an environment where (innocent and civilian) systems are not inadvertently affected while offering offensive cyber operators the opportunity to be distinct and proportional in their actions.

That same mutuality can be found when considering the norms on offensive cyber. There are responsibilities for states that possess and use cyber capabilities as well as for states who believe they have been attacked by other states' offensive cyber activities. The different pieces of guidance that can be found in the set of eleven norms are presented in Tables 2 and 3 respectively, with a distinction between encouraging and constraining actions.

The do's and don'ts outlined in Table 2 show that the current UN norms assign a range of responsibilities to any state involved in offensive cyber.

For instance, the UN norms constrain the use of offensive cyber by requiring operations to be targeted and to exclude effects on other states' critical infrastructure and CERTs, including through second- and third-order effects. The norms also require that tools and techniques need to be used in such a way that they do not proliferate any further, and vulnerabilities

Table 2: Guidance from the UN norms on responsibilities to states involved in offensive cyber.

Individual States should apply the following actions:

- Take reasonable steps within their capacity to end the ongoing activity in its territory.[39] (to prevent a potential internationally wrongful act[40]).
- Respect and protect human rights and fundamental freedoms, in particular the freedom of expression which includes the freedom to seek, receive, and impart information regardless of borders and through any media.[41]
- Put in place relevant policy and legislative measures at the national level to ensure that state-sponsored ICT activities that may impact the critical infrastructure or delivery of essential public services in another state conducted in accordance with international law and subject to comprehensive review and oversight.[42]
- Prevent the proliferation of malicious ICT tools and techniques.[43]
- Introduce measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity, and availability of systems and networks.[44]
- Put in place legal frameworks, policies, and programs to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution.[45]
- Distinguish their national CERT(s) from other arms of government.[46]

Individual States should refrain from the following actions:

- Carry out activities that threaten international peace and security or are harmful.[47]
- Practice arbitrary or unlawful mass surveillance.[48]
- Intentionally damage critical infrastructure or otherwise impair the use and operation of critical infrastructure to provide services to the public, including cascading domestic, regional, and global effects.[49]
- Conduct or knowingly support activity to harm the IT systems of CERT in recognition of their unique responsibilities and functions in managing and resolving ICT incidents.[50]
- Use their national CERT(s) to engage in international malicious activity.[51]

should not be used in a way that additionally compromise the confidentiality, integrity, and availability of ICT products. Also, the state authoring the operation should be able to end the activity once it appears to be threatening international peace and security and/or amounts to an internationally wrongful act.

The UN norms further state that the possession of offensive cyber capabilities comes with the responsibility to follow adequate policy and legislative measures to ensure that no operation will breach obligations under international law and to guarantee a form of review and oversight. They also set out the responsibility to not engage a state's national CERT in offensive cyber operations and to ensure a separation of staff, tools, and command and control.

The development of offensive cyber capabilities or attempts to acquire or procure access to third-party capabilities do not seem to be guided by the UN norms. In other words, states are currently free to pursue these assets.

The norms also extend duties to states that believe they have been attacked by an offensive cyber operation. They need to contact, consult, and inform the other states concerned, including the presumed author. They also have to make sure they have done their own due diligence regarding cybersecurity measures and incident response mechanisms. Finally, the norms indicate an affected state should "take a deep breath" and respond proportionally and in an informed manner.

Table 3: Guidance from the UN norms on responsibilities to states who fall victim to another state's offensive cyber.

States should:

- Consult among relevant competent authorities between the states concerned.[52]
- Consider all relevant aspects in their assessment of the incident. This can include the incident's technical attributes; its scope, scale, and impact; and the wider context, including the incident's bearing on international peace and security.[53]
- Take all appropriate and reasonably feasible steps to detect, investigate, and address the situation.[54]
- Notify the state from which the activity is emanating.[55]
- Take appropriate measures to protect its critical infrastructure and designate infrastructure and sectors it deems critical.[56]
- Classify ICT incidents in terms of their scale and seriousness.[57]
- Authorize national CERT(s) and put in place a national ICT-security incident management framework.[58]
- Respect and protect human rights and fundamental freedoms, in particular the freedom of expression which includes the freedom to seek, receive and impart information regardless of frontiers and through any media.[59]

States should not:

- Monitor all ICT activities within their territory.[60]

How each state fulfils these responsibilities is a matter of national policy and sovereign decision-making. It will differ among states based on factors such as political-military culture, national cyber and security context, and institutional arrangements of government. The UK and Australia, for instance, will have special duties to reassure friends and foes of their responsible conduct of operations given the integration of the national CERT and National Cyber Security Centre into, respectively, Government Communications Headquarters (GCHQ) and the Australian Signals Directorate (ASD). In Australia, ASD has the national mandate for developing tools, techniques, and procedures of offensive cyber that they then "offer" to Defense or a respective military command.[61] In the UK, together with the Ministry of Defence, Secret Intelligence Service, and Defence Science and Technology Laboratory, GCHQ coordinates the National Cyber Force, which is the only recognized body to conduct offensive cyber operations.[62]

Different Types of Offensive Cyber Operations in the Context of International Security

The UN cyber norms are a relevant mechanism to assess offensive cyber. They provide distinct guidance to states on their use of and any responses to the use of offensive cyber by others. The next thing to consider is the context in which offensive cyber capabilities are deployed, in particular situations that may constitute a threat to the maintenance of international peace and security.

Different perspectives address the strategic value of offensive cyber operations. Based on anecdotal evidence that is surfacing from past cyber operations, it appears that the cyber domain is a treasure trove for intelligence-collection activities such as intercepting communications and data, stealing high-value intellectual property, and pre-positioning for any potential future acts.

While debates continue as to whether cyber espionage meets the criteria of offensive cyber, in most cases state capabilities and agencies mandated with foreign (cyber) espionage are the same as, or closely connected to, those for offensive (military) cyber operations. In diplomatic practice, however, the use of cyber tools for intelligence purposes does not appear controversial or

discouraged.[63] Intelligence operations have only become problematic in situations in which they were discovered, exceeded a distinct political-military (information) purpose, for instance, in the case of cyber-enabled theft of intellectual property or created unintended physical effects.

Another use case is cyber operations that are part of a wider campaign of authorized military operations; they are one of the many "weapons"[64] that can be deployed both in the intelligence preparation of the battlefield[65] and for tactical operations. A well-known example of the latter is the cyber operation by the US, UK, and Australia against the Islamic State's propaganda network in 2016.[66] Also, recent Russian cyber operations as part of the military campaign against Ukraine, and earlier, in 2008 against Georgia, fit this category.

In the similar military context, there are several examples of standalone offensive cyber operations. The Olympic Games/Stuxnet operation attributed to the US and Israel against Iran's nuclear capabilities is an example that fits this label as does the use of offensive cyber capabilities to combat cybercrime and prevent terrorist use of the internet. The Australian government, for example, has declared a willingness to deploy their offensive capabilities to pursue overseas cyber criminals,[67] and the US conducted operations "to impose costs" on Russian-based ransomware groups.[68]

The last category of offensive cyber operations to carefully consider in the context of international peace and security is the use of cyber capabilities by security and intelligence agencies under domestic law and for national (public) security purposes.[69] In efforts to stem discontent, surveil political opposition, demoralize insurgency groups and control the flow of information and data in and out of the country, security agencies have imposed crude tactics that wouldn't be out of place in an inter-state conflict. Furthermore, states will be challenged in any claims of sole domestic effects of the use of cyber capabilities given the character of the networks and almost inevitable cascading effects outside their sovereign borders.

In these four situations, states make use of their offensive cyber capabilities in the pursuit of what can be legitimate national interests. In doing so, however, they may exceed the boundaries of responsible behaviour and create a threat to international stability. This then leads to the final question of how the UN norms can be applied. This requires a more detailed understanding of what tools, techniques, activities, and impact are out of bounds, and through which means and mechanisms offensive cyber acts can be verified.

Applying the UN Norms in Maintaining International Peace and Security

In conventional warfighting and peacekeeping, international legal concepts, thresholds of peace and conflict, and rules of engagement are relatively clear and established. The UN Security Council typically acts as the premier body to discuss issues related to the maintenance of international peace and security, including investigations into international disputes, recommendations to resolve tensions, and the determination of the existence of a threat or acts of aggression. The Council can also decide to impose sanctions or authorize military responses.[70]

Through these functions, the Council has been applying rules of international law alongside a wide variety of norms of responsible state behavior, such as committing to the responsibility of humanitarian intervention and mandates around the protection of civilians. The UN General Assembly, where all international cybersecurity debates have so far taken place, can only make non-binding recommendations and, in practice, the nature of the General Assembly's First Committee deliberations have been largely conceptual and legalistic rather than issue- or incident-specific.

During its non-permanent term on the UNSC in 2020-21, Estonia has been fronting a series of so-called Arria formula meetings.[71] These are informal sessions intended to engage stakeholders outside of the UN system or to raise issues that have not yet found their way to the formal agenda of the Security Council. These are valuable steppingstones to arrive at a future situation where an international body such as the Security Council will express an opinion about an act of offensive cyber in terms of its legality and legitimacy. For now, Russia, China, and their allies do not see a role for the UN Security Council on international cyber matters.[72] This aligns with their effort to prevent the acknowledgment of "the militarisation of cyberspace."

For the purpose of arms control, disarmament, and conflict prevention, the UN and various regional organizations have mechanisms in place for states to report on their military capabilities, doctrines, and decision-making, which are monitored by international secretariats, civil society organizations, and academia.[73] Similar activities have started to emerge for cyber capabilities that may jeopardize international peace and security including offensive cyber operations. Examples include the cyber operations[74] and significant cyber incident[75] trackers, cyber power, and capability indices,[76] and assessments of nations' international cyber strategies.[77] Yet, these have not yet reached a level of maturity to consequently affect national decision-making and offer a robust form of international accountability.[78]

The non-tangible and yet-too-difficult-to-verify character of cyber operations is a significant hindering factor in this accountability effort. Also, the dominant roles of intelligence agencies and the use of proxy actors add to the level of secrecy surrounding state cyber capabilities. Nonetheless, a gradually growing body of public government documentation is emerging that allows assessments to be made. These include cybersecurity strategies, operational concepts for cyber commands, and military cyber-related Standard Operation Procedures (cyber-SOPs). Confidence-building measures promoted by the UN, as well as several regional organizations, are promoting the sharing of official, but unclassified documents like these.

There is a pivotal role for Track Two actors such as academia, think tanks and civil society organizations to keep pushing states at the national and operational level to exercise greater transparency and to expose and report on real-life incidents, compare these with public documents, and offer informed assessments of the responsible and irresponsible nature of specific offensive cyber activities.

CONCLUSION

The UN norms of responsible state behaviour in cyberspace do not discourage, let alone stop, states from developing or procuring cyber capabilities. In fact, it is most likely that more states will pursue national cyber capabilities for either domestic security purposes or in light of geo-economic competition.

However, this does not necessarily lead to an offensive future. Ever since international ICT security was put on the UN agenda as a topic in 1998, the world's major cyber powers, including the US, Russia, and China, have shown an interest in developing and committing to certain basic minimum rules.

The UN norms provide relevant guidance to states in terms of their responsible possession and use of offensive cyber capabilities. While they are anything but complete and unambiguous, collectively the current set of 11 norms provides a distinct direction. It shows what activities, effects, and practices the international community does not want to see occurring.

While norms are occasionally violated, the general applicability of the 11 UN norms is not disputed. Further work is required to marry UN language around "maliciousness" with offensive cyber, develop operational guidance, and find mechanisms to assess states' on-going observance.

Responsible forms of offensive cyber will not be recognized by or achievable for everyone and most likely remain the business of a limited group of states that show a political interest in projecting power in cyberspace, have a digital and tech-enabled economy and can employ operators with sophisticated technical skillsets. More fundamentally, these frontrunners will benefit from setting the bar of responsible state behavior high as their own capabilities grow and professionalize.

An elevated bar for states to responsibly possess and use offensive cyber capabilities should create an environment where states can use these tools and assets for legitimate national interests but without jeopardizing international peace and security, and societal trust and confidence in ICTs and the digital domain.

APPENDIX

The full text of the UN norms of responsible state behavior in cyberspace, as contained in UN General Assembly Resolution 70/237 (2015).

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

NOTES

1. Statement made plus author's conversation with Microsoft's global diplomacy team.
2. Microsoft, Protecting people in cyberspace: The Vital Role of the United Nations in 2020, 2, https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf.
3. UN General Assembly, Resolution 73/27, operative clause 5, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement.
4. Australian Strategic Policy Institute, The UN norms of responsible state behaviour in cyberspace, explainer video,https://ad-aspi.s3-ap-southeast-2.amazonaws.com/2020-09/cybernorms_ENGLISH.mp4.
5. UNOEWG (2021), Summary report of the informal intersessional consultative meeting, December 2-4, 2019, https://front.un-arm.org/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf.
6. See for example: Jim Lewis, Toward a More Coercive Cyber Strategy: Remarks to U.S. Cyber Command Legal Conference, March 4, 2021 https://www.csis.org/analysis/toward-more-coercive-cyber-strategy; Ciaran Martin, Cyber 'Deterrence': A Brexit Analogy, January 15, 2021, https://www.lawfareblog.com/cyber-deterrence-brexit-analogy; Global Commission on the Stability of Cyberspace, Advancing Cyberstability; Final report, November 2019, https://www.whitehouse. gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/, see chapter 2 for a definition of cyberstability as intended here.
7. Government of the United States, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.
8. Ibid.
9. Government of New Zealand, New Zealand condemns malicious cyber activity by Chinese state-sponsored actors, July 19, 2021, https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors.
10. US ("The PRC's pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world" https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/); UK ("The UK is calling on China to reaffirm the commitment made to the UK in 2015 and as part of the G20 not to conduct or support cyber-enabled theft of intellectual property of trade secrets" link); Australia ("Australia calls on all countries – including China – to act responsibly in cyberspace. China must adhere to the commitments it has made in the G20 and, bilaterally, to refrain from cyber-enabled theft of intellectual property, trade secrets and confidential business information with the intent of obtaining competitive advantage," https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china); EU ("We continue to urge the Chinese authorities to adhere to these norms and not allow its territory to be used for malicious cyber activities, and take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation," https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/; NATO ("we call on all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace," NATO - News: Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise, 19-Jul.-2021).
11. UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), A/70/174, paragraph 13(b), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.
12. UN General Assembly, Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (2021), paragraph 30(d).
13. Tom Uren, Bart Hogeveen, and Ferus Hanson, Defining offensive cyber capabilities, ASPI. Memo for the Global Commission for the Stability in Cyberspace, July 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

NOTES

14. For Russia, see for instance, Janne Hakala and Jazlyn Melnychuk, Russia's strategy in cyberspace. NATO Strategic Communications Centre of Excellence, June 2021, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021. pdf; for China, see for instance: The Guardian, Experts say China's low-level cyberwar is becoming severe threat, September 23, 2021, https://www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat; for Iran, see for instance, US Congressional Research Service, Iranian offensive cyber-attack capabilities, January 2020, https://sgp. fas. org/crs/mideast/IF11406.pdf.
15. For instance, see, Josh Gold, A cyberspace FIFA to set rules of the game? UN states disagree at second meeting. CfR Net Politics, March 2, 2020, https://www.cfr.org/blog/cyberspace-fifa-set-rules-game-un-states-disagree-second-meeting.
16. ASPI-ICRC workshop with Australian government representatives, September 2021, Report forthcoming.
17. Statement by the delegation of the Republic of Indonesia on behalf of the Non-Aligned Movement, First Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, September 9, 2019, PERMANENT MISSION OF THE REPUBLIC OF INDONESIA, TO THE UNITED NATIONS, NEW YORK (kemlu.go.id).
18. Bart Hogeveen, *The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for member states of ASEAN,* Australian Strategic Policy Institute, March 2022, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.
19. Elaine Korzak, UN GGE on Cybersecurity: The end of an era? *The Diplomat*, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.
20. Bart Hogeveen, Six years in the making: UN reaches global cyberspace consensus, *ASPI Strategist*, March 26, 2021, https://www.aspistrategist.org.au/six-years-in-the-making-un-reaches-global-cyberspace-consensus/.
21. Josh Gold, Unexpectedly all UN countries agreed on a cybersecurity report. So what? *Council for Foreign Relations,* March 18, 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.
22. Hogeveen, Six years in the making: UN reaches global cyberspace consensus.
23. UN General Assembly Resolution 75/240, January 4, 2021, operative clause 1, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement.
24. Uren, Hogeveen, and Hanson, Defining offensive cyber capabilities.
25. UN General Assembly, Resolution 70/237.
26. Bart Hogeveen, The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for member states of ASEAN, Australian Strategic Policy Institute, forthcoming.
27. During the 1999 NATO intervention in Kosovo, NATO networks were targeted through a Denial-of-Service attack (Christine Hegenbart, Semantics matter. NATO, cyberspace and future threats, NATO research paper, July 2014, https://www.ndc.nato.int/news/news.php?icode=701#) and the US military reportedly considered hacking into Serbia's central bank and degrading Serbia's financial systems (Julian Border, Pentagon kept the lid on cyberwar in Kosovo, *The Guardian,* November 9, 1999, https://www.theguardian.com/world/1999/nov/09/balkans); During the second Chechen war, the Russian military sought to disrupt websites and information databases of its opponents (Kenneth Geers, Cyberspace and the changing nature of warfare, NATO CCDCOE, keynote speech, https://csl.armywarcollege.edu/SLET/mccd/CyberSpace-Pubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf; and Timothy L. Thomas, Information warfare in the second (1999-present) Chechen war: Motivator for military reform? 2003, https://community.apan. org/cfs-file/__key/docpreview-s/00-00-08-52-36/2002_2D00_01_2D00_01-Information-Warfare-in-the-Second- _2800_1999_2D00_Present_2900_-Chechen-War-_2800_Thomas_2900_.pdf.
28. Allegedly, the US government's NSA and CIA together with Israeli intelligence services developed the Stuxnet virus to degrade the industrial control systems of Iran's nuclear facility in Natanz (Mariusz Antoni Kaminski, Operation Olympic Games. Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme, in: Security and Defence Quarterly, 2020:29(2): 63-71, https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html.
29. This refers to leaked documents by former NSA contractor Edward Snowden on the US NSA's surveillance activities. They disclosed the tools and techniques that were being used targeted systems, internet providers, and other platforms and encryption keys they had managed to break; *Lawfare*, Snowden revelations, https://www.lawfareblog.com/ snowden-revelations.

NOTES

30. UNGGE (2021), paragraph 71 (f).
31. UNOEWG (2021), Summary report of the informal intersessional consultative meeting, December 2-4, 2019, LetterF702.dot XP (un-arm.org)
32. Bart Hogeveen, "Which practices help us maintain a secure cyberspace in the Asia Pacific?" APNIC blog, November 26, 2020, https://blog.apnic.net/2020/11/26/which-practices-help-maintain-secure-cyberspace-asia-pacific/.
33. GGE report, para 18.
34. A scan of the 2021 reports (which includes relevant passages of previously agreed text) do not show terms that explicitly relate to "offensive" and "offensive cyber operations" or "capabilities."
35. UNGGE (2021) and UNOEWG (2021).
36. UNGGE (2021) and UNOEWG (2021).
37. Lesley Seebeck, Grey zone strike means cyber war, in *Australian Financial Review*, June 24, 2020, https://www.afr.com/policy/foreign-affairs/grey-zone-strike-means-cyber-war-20200623-p5556b.
38. UNGGE (2021), paragraph 18.
39. UNGGE (2021), paragraph 30(a)
40. An Internationally Wrongful Act is an act that is (a) attributable to a state, and (b) a breach of a rule of international law. See: Francois Delerue, Cyber operations and international law, 2020, chapter 5: Internationally wrongful acts: cyber operations breaching norms of international law.
41. UNGGE (2021), paragraph 13(e).
42. UNGGE (2021), paragraph 46.
43. UNGGE (2021), norm 13(i), paragraph 56.
44. UNGGE (2021), paragraph 58(c).
45. UNGGE (2021), paragraph 62.
46. UNGGE (2021), paragraph 68.
47. UNGGE (2021), paragraph 20.
48. UNGGE (2021), paragraph 37.
49. UNGGE (2021), paragraph 42.
50. UNGGE (2021), paragraph 65.
51. UNGGE (2021), paragraph 67.
52. UNGGE (2021), paragraphs 23 and 24.
53. UNGGE (2021), paragraph 24.
54. UNGGE (2021), paragraph 29.
55. UNGGE (2021), paragraph 30(c).
56. UNGGE (2021), paragraph 48.
57. UNGGE (2021), paragraph 50.
58. UNGGE (2021), paragraph 68.
59. UNGGE (2021), norm 13(e).
60. UNGGE (2021), paragraph 30(a).
61. Australian Signals Directorate, Annual Report 2019-20, chapter 3: offensive cyber operations – performance analysis, Offensive cyber operations - performance analysis | Transparency Portal.
62. UK government, National Cyber Force explainer, December 2021, Microsoft Word - Force Explainer 20211213 FINAL.docx (publishing.service.gov.uk).
63. For instance, see: Russell Buchan and Inaki Navarrete, Cyber espionage. Oxford bibliographies, Cyber Espionage - International Law - Oxford Bibliographies; Ilina Georgieva, The unexpected norm-setters: Intelligence agencies in cyberspace, in Contemporary Security Policy, vol. 41, 2020, issue 1, https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677389.

NOTES

64. For an overview of offensive cyber capabilities that nation states might deploy, see: Ciaran Martin, Cyber-weapons are called viruses for a reason: Statecraft and security in the digital age. Inaugural lecture, King's College London, November 2020, https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf.
65. See, for instance, U.S. Army, Army Technical Publication 2-01.3, *Intelligence Preparation of the Battlefield*, March 1, 2019, appendix D: IPB Cyberspace Considerations, https://home.army.mil/wood/application/files/8915/5751/8365/ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield.pdf.
66. Stephanie Borys, Australian cyber soldiers hacked Islamic state and crippled its propaganda unit – here's what we know, ABC News, December 18, 2019, https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426.
67. Australian Minister of Defence, Australia continues to combat foreign cybercriminals, media release, December 2, 2020, https://www.minister.defence.gov.au/minister/lreynolds/media-releases/australia-continues-combat-foreign-cybercriminals.
68. Julian E. Barnes, US military has acted against ransomware groups, General acknowledges, *The New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.
69. For instance, see Dien Nguyen An Luong, How the Vietnamese state uses cyber troops to shape online discourse, in ISEAS Perspective 2021/22, March 3, 2021, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong/.
70. UN Security Council, Functions and Powers, Functions and Powers | United Nations Security Council.
71. ERR, UN Security Council reaffirms important of cyberstability, May 23, 2020, https://news.err.ee/1093658/un-security-council-reaffirms-importance-of-cyberstability.
72. What's in blue: Arria-formula meeting on "preventing civilian impact of malicious cyber activities," Security Council report, December 19, 2021,UN Security Council reaffirms importance of cyberstability | News | ERR.
73. For example, one can look at the work of SIPRI (SIPRI yearbook) and Crisis Group.
74. Council on Foreign Relations, Cyber operations tracker, https://www.cfr.org/cyber-operations/.
75. Centre for Strategic and International Studies, Significant cyber incidents, Significant Cyber Incidents | Center for Strategic and International Studies (csis.org).
76. For instance, see Belfer Center, National Cyber Power Index 2020, https://www.belfercenter.org/publication/national-cyber-power-index-2020; IISS, Cyber capabilities and national power, June 28, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
77. For instance, see the Cyber Diplomacy research papers on China, Russia, India, Latin America, and Southeast Asia from the EU Cyber Direct (Cyber Diplomacy) project, https://eucyberdirect.eu/research?category=research-papers.
78. ASPI and ICRC, Report on workshop, forthcoming.