ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY

Edited by
Eneken Tikk and Mika Kerttunen

First published 2020

ISBN13: 978-1-138-48901-1

Chapter 30

THE ROLE OF THE UN SECURITY COUNCIL IN CYBERSECURITY

International peace and security in the digital age

Eneken Tikk and Niels Nagelhus Schia

The OA chapter is funded by NUPI

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

30

THE ROLE OF THE UN SECURITY COUNCIL IN CYBERSECURITY

International peace and security in the digital age

Eneken Tikk and Niels Nagelhus Schia

On the 75th anniversary of the United Nations, the UN Security Council is faced with difficult questions about its efficacy, relevance, and legitimacy. The leading powers and the permanent members (P5) of the Security Council – China, France, Russia, the UK and the USA – are drawn into a heavy contest over the world order. Power lines are (to be) drawn in an increasingly digital, interconnected and multi-stakeholder society. So far, despite the language from heads of states, global media houses and from leaders of international organizations, including NATO and the UN, none of the P5 countries has brought cyber to the UNSC. Other countries – for instance, Lithuania and the Netherlands – have considered introducing cybersecurity issues to the Council, but no action has followed. One of the most recent members-elect, Estonia, has pledged to take up the issue.

To stay relevant and act upon its responsibility for international peace and security, the Security Council will have to establish itself vis-à-vis cyber issues. The goal of this chapter is to examine why and how. To what extent do questions pertaining to digital threats and cybersecurity fall within the mandate of the Council and what could it address given the politically tense times among the P5? The analysis of the role of the UNSC in cybersecurity seems to be a blind spot in scholarly literature on international peace and security. Recently, leading scholars took stock of the relevance of the UNSC and its most pressing challenges in the twenty-first century in an edited volume of one thousand pages (von Einsiedel et al., 2016). However, neither information and communication technology nor cybersecurity are mentioned anywhere in that volume.

Essential to the discussion of the possible role of the Security Council in cybersecurity is how current international cyber affairs will be qualified in the context of the UNSC mandate: have contemporary uses of ICTs emerged as significant, new and urgent threat to the peace (Simma, 2012, p. 785)? Are there any disputes present among UN member states that, if continued, are likely to endanger the maintenance of peace (UN Charter, 1945, Art. 33)? Is the time ripe for the Council to consider 'all things digital' (Kaljulaid, 2018)? If so, despite the known limitations on its operability, a number of ways are open for the Council to become engaged. If not, any direct role of the Security Council must be dismissed. In this case, however, one must critically (re-)assess the relevance of the whole UN First Committee cybersecurity dialogue that is premised on the potential threat to international peace and security resulting from state use of ICTs.

Taking a stand on an issue beyond any particular territory or event is not unprecedented. With Resolutions 1373 and 1540 the Security Council addressed a more general and abstract issue that has led some authors to conclude that the Council has assumed a law-making role. By declaring international terrorism as a threat to international peace, the Security Council imposed general obligations on all States in a context not limited to a particular country (de la Serna Galvan, 2011, p. 148).

After a discussion of the current cybersecurity situation, we will proceed with a verdict on ICTs as a threat to peace and security, calling for a corresponding conversation between states, potentially at an invitation of a Security Council member state. The chapter continues with a discussion of ways in which the Security Council could become involved in matters of cybersecurity, briefly discussing likely applicable factors of limited operability. Finally, some related considerations for states are put forward.

Three outlooks on peace

The UNSC is the executive decision-making arena of the United Nations and the world's most important international decision-making body with the primary responsibility of maintaining international peace and security. The Council's legitimacy depends on the maintenance of its original purpose as set out in the UN Charter which, as Fassbender (2012) notes, is hard to verify or falsify. What characterizes this body is not only that its decisions have far-reaching effects across the world, but also that its decision-making process is affected by both the macroeconomics of power and the micro-politics of the informal processes (Schia, 2017, p. 55 and 2018, p. 122). This means that its effectiveness in decision-making is highly dependent of the climate between the Permanent Members.

After a honeymoon period from 1945 to the mid-1950s, the Security Council froze in the icy relationship between the United States and the Soviet Union. In the Cold War reading, of which the U2 incident and the Cuban Missile Crisis offer illustrations, the Security Council's role in world politics remained modest and passive. Wuthnow (2011) notes that since the fall of the Berlin Wall, the Council has met three times as often as it did during the Cold War. During the same period, it passed more than ten times more resolutions under Chapter VII than it did between 1946 and 1989 (Wuthnow, 2011, p. 4). The '1962 Outlook' on the Security Council would involve low expectations, where the Council remained largely detached from the world affairs and would not be seen as a source of inspiration for peace and stability. Fassbender summarizes that the expectations of the Security Council were so low that doing nothing was an achievement on its own (Fassbender, 2012, p. 53).

After the Cold War, new kinds of conflicts and broader security concerns were increasingly included on the Security Council agenda, many of them without immediate peace and security implications. The Security Council became regarded as a forum to uphold the purposes and principles of the UN, as enshrined in the UN Charter or the 1970 Friendly Relations Declaration. The '1992 outlook' has the Security Council both removing and preventing threats to peace, thereby occupying the most encompassing, powerful, and direct mandate to shape stability and order in the world. The Council has demonstrable achievements to feed such high expectations. In the context of the protection of civilians, the Council recognized 'the importance of a comprehensive, coherent and action-oriented approach, including in early planning, of protection of civilians in situations of armed conflict' and stressed

> the need to adopt a broad strategy of conflict prevention, which addresses the root causes of armed conflict in a comprehensive manner in order to enhance the protection of civilians on a long-term basis, including by promoting sustainable development, poverty eradication, national reconciliation, good governance, democracy, the rule of law and respect for and protection of human rights.
>
> *(S/RES/1738)*

Furthermore, the Council became concerned about 'deliberate attacks in violation of international humanitarian law' (S/RES/1738), stating that states "bear the primary responsibility to respect and ensure the human rights of their citizens, as well as other individuals within their territory as provided for by relevant international law' (S/RES/2150). It put up strong opposition to impunity for serious violations of international humanitarian law and human rights law and emphasized the responsibility of States to comply with their relevant obligations to end impunity (S/RES/2150). Naturally, these lines remain in the context of the Security Council's mandate. However, they leave little question as to the Council's attitude towards international law, wherever it becomes seized of the matter.

More recent years, however, have shown new signs of an inefficient Security Council and a suboptimal working climate between its permanent members. Tensions have escalated with the civil war in Syria, the annexation of Crimea, accusations of interference in national elections and a combination of trade war, power politics, and old school geopolitics. The UNSC has not only become characterized by a difficult working atmosphere, but there is also a new trend in international relations, whereby decisions about international peace and security are being taken outside of the UN and there is an 'emerging reality that the most important challenge to international peace and security is one in which the Security Council is not present, and arguably not relevant' (Jones 2016, p. 802–804).

As superpower rivalry deepens, the question of the Council's efficacy re-emerges. Several attempts have been made, without success, over the past years to make the Council more inclusive and better responsive to the international community's needs (Simma, 2012; Fassbender, 2012). Alongside the expectations that have been made possible by the nearly 25 years of active involvement, the Council must face criticism about having become a vehicle for the USA and its allies to seek to punish and coerce regimes with which Russia and China maintain close relations (Wuthnow, 2011, p. 5). Similarly, Russia and China can be criticized for emphasizing hard security and absolute sovereignty over human security and human rights. Accustomed to the absence of hard conflict, the international community requires leadership in maintaining peace. It is unclear, both in the context of cybersecurity as well as in general security affairs, whether the Security Council will rise to this task.

In any case, the 1962 outlook, based on the realities of the Cold War, hardly satisfies the hopes of the international community of 2022. The 1992 outlook, in contrast, may put too high hopes on the Council. The central question in this chapter is the position that the Security Council could assume in international cyber affairs.

International cyber affairs in the context of peace and security

The (hypothetical) threat and the (quasi-) conflict

The question of the Council's involvement is more than open. When looking at statements relating to cyber threats, it is not unreasonable to assume an active role of the UN Security Council in international cyber affairs. The General Assembly has called on UN member states 'to be guided in their use of recommendations of the Group of Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (A/RES/71/28, para 1a). According to this report, '[t]he use of ICTs in future conflicts between States is becoming more likely', '[t]he risk of harmful ICT attacks against critical infrastructure is both real and serious' and states are 'rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy' deriving from the difficulty of attributing the source of an ICT incident (UN A/70/174, paras 4, 5 and 7). Table 30.1 summarizes the argumentation (and consensus) on threats that uses of ICTs *may* pose to international peace and security in the three GGE reports.

However, this table contains a number of hypotheticals and the lack of any definitive action to follow up on these innovations. The GGE has iterated several times that the growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services. As the GGE in 2013 concluded, 'any ICT device can be the source or the target of misuse'. The Group identified global connectivity, vulnerable technologies and anonymity as facilitators of the use of ICTs for disruptive activities. It noted that the 'rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security' (GGE, 2013). Despite these pointers, the Group has not warned about the growing dependence on ICTs.

Furthermore, the Group has expressed concern that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure, and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security (GGE, 2010, p. 8). Not much has been undertaken to build or restore this trust.

In addition to the UN GGE, the Secretary-General has elaborated the cyber threat. In his address to the General Assembly in 2017 Secretary-General Antonio Guterres referred to cyber war as 'a less and less a hidden reality – and more and more able to disrupt relations among States and destroy some of the structures and systems of modern life' (United Nations Secretary-General, 2019). NATO's Secretary-General Jens Stoltenberg also highlighted that cyber-attacks could be 'as damaging as conventional attacks', susceptible of 'inflicting billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and have a crippling impact on military capabilities' (Stoltenberg, 2019). Joseph S. Nye highlights how the potential attack surface will expand dramatically and provide opportunities for both private and interstate conflict (Nye, 2018, p. 7).

Despite the strong language pointing to international peace and security concerns, neither the UN GGE nor any other actor has been able to assert, in the context of state uses of ICTs, the acuteness of the politico-military threat, let alone a threat to international peace and security, breach of the peace or act of aggression that the UN Charter points to. Importantly, none of the states participating in the GGE has deemed it necessary to bring the issue to the UN Security Council.

It is equally problematic to discern immediate peace and security concerns from known or alleged state-sponsored cyber operations. Of known or allegedly state-sponsored cyber operations, the vast majority are cyber espionage. The rest, around 10% of all the catalogued incidents, have relatively low effects, such as website defacement, denial of service, in some cases data manipulation and, in a very few cases, sabotage and physical damage (Council of Foreign Relations. 2019; CSIS (2019); Maness, Valeriano and Jensen, 2019).

Table 30.1 Summary of the UN GGE 2010, 2013 and 2015 reports argumentation of the threats

2010	*2013*	*2015*
	The absence of common understandings on acceptable state behaviour with regard to the use of ICTs increases the risk to international peace and security.	There are disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by state and non-state actors.
Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future.	Terrorist groups use ICTs to communicate, collect information, recruit, organize, plan and coordinate attacks, promote their ideas and actions and solicit funding. If such groups acquire attack tools, they could carry out disruptive ICT activities	The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.
There is increased reporting that states are developing ICTs as instruments of warfare and intelligence, and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception		A number of states are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy.
The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.	The expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption.	The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a state. The risk of harmful ICT attacks against critical infrastructure is both real and serious.
	The rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security.	
The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.	States are concerned that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security.	

2010	*2013*	*2015*
The varying degrees of ICT capacity and security among different States increases the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.	Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world. Malicious actors exploit networks no matter where they are located. These vulnerabilities are amplified by disparities in national law, regulations and practices related to the use of ICTs.	

Source: Authors' compilation from the reports

Furthermore, the vast majority of known incidents reflect established dyadic rivalries where, if anything, they point to a slight de-escalation in means and methods of politico-military confrontation.

Effect-creating cyber incidents that have taken place with some state involvement in the past two decades can be characterized primarily as low-intensity conflict. Originating in US military doctrine, it has analytical value in the context of cyber and hybrid warfare:

> Low intensity conflict is a political-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideologies. Low intensity conflict ranges from subversion to the use of armed force. It is waged by a combination of means, employing political, economic, informational, and military instruments.
>
> *(United States of America, 1996).*

Taylor (1988, pp. 5–6) characterizes low intensity conflict as a situation where

> interests are contested; organized violence is used to effect or influence outcomes; all elements of national power are employed; the military dimension is employed primarily for its political, economic and informational effect; military violence is employed indirectly or limited by time and objective.

The fact that cyber operations often do not meet the predicted thresholds of doom and destruction, deserves special attention in the context of international peace and security. The question becomes whether, due to their relatively low effects, cyber incidents should be disqualified as 'conflict', or is the discussion of conflict to be extended to struggles that remain, perhaps deliberately, below the threshold of use of force, yet constitute a new trend in state power projection. Most cyber incidents with known or suspected state involvement have occurred under explicit or implicit endorsement of the permanent members of the UNSC.

What are the prospects?

Estonia, one of the newest additions to the Council, has flagged the question of cybersecurity as part of their candidacy campaign. The President of the Republic of Estonia has expressed the intent to raise issues of cybersecurity:

> all topics concerning cybersecurity and artificial intelligence must be brought to the Security Council's table. Because the international legal space is showing a clear developmental delay in the field.... Estonia is planning to make a contribution namely to finding a solution to problems concerning cyberthreats.
>
> *(Kaljulaid, 2018)*

The Estonian President has further elaborated on the plan, addressing the 73rd Session of the UN General Assembly:

> Small countries have no time for small objectives – our aim is, among other issues, to bring all things digital to Security Council – cyber risks are something Estonians as citizens of a fully digitized state understand better than most. We want to offer our perspective to make sure that human beings remain safe in this new world were cyber related threats compound with conventional ones.
>
> *(Kaljulaid, 2018)*

Indeed, ICTs constitute a pervasive technology that underpins not just advances in areas like materials, space, nuclear and biotechnologies (UNGA 1990). ICTs are also central to economic, societal, political, and military controls. ICT's omnipresence makes the currently 4.4 billion users (that is, over half of the world's population) online both recipients and potential sources of potentially destabilizing and security-endangering use of ICTs. However, is that enough of a reason for the Security Council to get involved in the discussion?

Accomplishing the Estonian endeavour is a challenge. Moscow and Washington, the leading powers in the cyber arms control dialogue, have remained silent on this particular issue. Despite making clear and frequent references to the threats related to the proliferation and certain uses of ICTs, neither the Russian Federation nor the USA have deemed it necessary to bring the matter to the attention of the Council. After two decades of expert discussions and heavy emphasis on arms control, this flags up the question of the real urgency and acuteness of the cyber threat.

It is also well acknowledged that the P5 hold fundamentally different positions on key aspects of cybersecurity. While the US, UK, and France, in general, share the same views on cybersecurity, China and Russia take a different position. These differences revolve around control of information and questions pertaining to sovereignty. While China and Russia emphasize the rights for states to protect their 'cyberspace' and 'information and media spheres', Western states fear that such rights will be used to justify surveillance, censorship, and repression in authoritarian states. Thus, by taking cybersecurity to the UNSC, Western states share a fear of opening a Pandora's box where already established rights concerning freedom of speech and human rights may be weakened. (For further details, see Tikk and Kerttunen 2018.) Thus global cyber governance and the role of the UNSC seem to hobble by an increasingly contentious debate that are i) obscured by attribution difficulties and the low-intensity character of cyber incidents ii) made difficult by political disagreements between P5, and iii) by an obfuscated situation concerning what it is that needs to be governed, the data or how to use the Internet.

However, the prospect may be improving, especially since Russia has taken a step towards a 'cyber-UNGA' with the OEWG. Getting the Security Council interested in cybersecurity issues is more in alignment with US interests than Russian aspirations. With the threat being unclear, the Council can embark on the US-championed proposition that the use of ICTs is to be guided under international law, while it harder to imagine an angle that would lead the Council support the proposition of *lex specialis*.

The elevated status of the P5, with veto rights and the ability to make binding decisions, may be hampering the Council from dealing with cybersecurity. A premature discussion in the UNSC could leave the P5 in the trenches, where China and Russia would welcome international regulations that strengthen cyber sovereignty, while the USA and the UK would be very cautious about such regulation. Ironically, compared to the OEWG, the UNGGE itself can be construed as a model of the Security Council: it involves experts from the P5 and, initially, it started out with the total of 15 members selected on the basis of equitable geographical distribution. As a 'light version' of the UNSC, the GGE could be an easier place to discuss new norms at a level without the commitments which are needed in order to reach consensus in the UNSC. But the recommendations of the GGE do have a stronger status than most other groups of experts in the UN as they have been endorsed by the Group of Twenty (G20). In this way, the discussions in the GGE could be regarded as a stepping stone towards a UNSC discussion.

Despite lacking a hard-grade threat factor, state-sponsored cyber incidents constitute an alarming practice. Attacks against critical infrastructure are particularly worrisome because societal and civilian life is dependent of those systems and services. Cyberattacks directed towards electric power grids and power supplies such as the attacks on Ukraine in 2015 and 2016 may knock power offline and in turn knock out businesses and other vital societal systems. The second category concerns telecommunications. If telecommunications are turned offline or made inaccessible, the Internet will be offline and there will be no free flow of commodities and services – again businesses and other vital societal systems will be impaired. This has also been used by authoritarian regimes to control the public during politically sensitive events such as the 2010 election in Myanmar and the election in DR Congo in 2018. An example is also a ransomware attack on Baltimore's city government in the USA in May 2019, where EternalBlue, also used in WannaCry and NotPetya, shut down emails and systems allowing citizens to pay water bills, purchase homes, etc. The third category of attacks concern international financial systems like SWIFT (Society for Worldwide Interbank Financial Telecommunication) which interconnect banks around the world. During a series of cyberattacks on the SWIFT banking network in 2015 and 2016, millions of dollars were stolen, including a 101 million theft from the Bangladesh central bank. Through cyberattacks on global financial systems, banks that have taken the necessary security precautions may also become compromised through smaller banks in countries with lower standards on cybersecurity, national policy, and regulations. What is common in these attacks is that they hit the nervous and life-sustaining systems of modern societies: they disturb the anticipated and vital flows of information, literally, and goods and services. They can also destabilize peaceful international relations and can escalate existing conflicts.

Of further potential is a discussion of threats to democracy manifested in manipulation of democratic processes. The Council has, in past decades, adopted resolutions about the restoration of democracy (S/RES/948), endorsing the results of free and fair elections (S/RES/960), civilian policing (S/RES/1212), and facilitating a comprehensive political dialogue (S/RES/1040). Whether the development or uses of ICTs constitute a threat to the peace or endanger the maintenance of the peace, is the main question of this book that cannot be resolved on the basis of the evidence and claims presented so far. It remains subject to further debate on whether the international community is willing to tolerate the economic and political struggles between the USA and its allies on the one side, and the Russian Federation and China on the other. As seen from the permanent members' perspective, such struggles should be considered normal in contemporary world politics. Whether others agree, remains to be discussed. There are several ways for the Security Council to become part of this conversation.

There are also some precedents for the theme being discussed under the aegis of the Council. Spain and Senegal made an attempt in November 2016 to get the Council involved in cyber security beyond the terrorism-related resolutions where cyber security is increasingly incorporated. They initiated and chaired an open Arria-meeting on cyber security – these are informal meetings the UNSC can arrange, mainly to meet with other delegations or NGOs or special representatives, and to discuss topics in a less binding manner.

The 2016 meeting included governments, organizations, civil society, and the private sector and sought to broaden the UNSC discussion on the matter by focusing on states and their potential use of cyberattacks and ICTs in political or military tensions, as well as the need to protect ICT-dependent critical infrastructure (What's in Blue, 2016; UNIDIR 2017, p. 25). At this meeting Council members were encouraged to improve ways of assessing vulnerabilities and preventing cyberattacks, to develop national strategies and policies, to commit to international cooperation, and to emphasize multi-stakeholder partnerships. Furthermore, the Arria-meeting questioned whether the Council itself was receiving appropriate information on two important aspects: i) on how ICTs can be used in emerging political and military tensions; and ii) on how the Council can contribute to mitigating these security implications.

In 2017, another ICT-related Arria-meeting was held, this time on 'hybrid wars as a threat to international peace and security'. The meeting was chaired by Ukraine and included discussions on cyber technologies, interference with political processes, disinformation and international peace and security (UNIDIR 2017, p. 25). Further, the UNSC's work on counter-terrorism there has been some aspects pertaining to ICTs included in resolutions. Resolutions 1267 (1999) and 1373 (2001) which constitute the framework for this work explicitly mentions terrorist use of ICTs (UNIDIR 2017, pp. 38–42).

Considerations for governments

None of the permanent members has taken the cybersecurity issue to the Security Council, despite their deep investment in the cyber arms control dialogue for over two decades. While changes in the attitudes of some of the P5, especially China and France, cannot be ruled out, it is more likely that the issue of cybersecurity ends up in the Security Council Chamber via a non-permanent member, another UN member state, the General Assembly or the UN Secretary-General. Without much prospect of the permanent members taking up the issue, it falls upon all interested governments to develop a convincing account of the Security Council's role and the expected outcome of its involvement.

The permanent members are split in their views about the role of ICTs in social, economic, political, and military affairs. Consequently, informal consultations and meetings are a more fruitful way ahead, at least in the coming two years where the new UN GGE and OEWG are in session. Whether the P5 will stand up to a sense of shared stewardship and global responsibility, being potentially accepted as the world police, remains to be seen. Meanwhile, as long as the rest of the world acts like the periphery, they will be treated as such. Breaking the empty cycle of cyber talks requires strong leadership and strategic vision, which can be developed gradually via a series of examinations of state uses of ICTs, their implications as well as underlying causes, to decide whether and how any of these do or can endanger peace.

The Open-Ended Working Group that parallels the UN GGE has been dubbed the cyber-UNGA (Krutskikh 2019). The General Assembly remains a forum for states to draw attention to ongoing cyber incidents as well as trends in the state development and use of ICTs. A worthwhile exercise for all governments interested in the progress of international cybersecurity solutions is to consider whether the UN GGE has been run as a suboptimal substitute to the UN Security Council in this area. This question has both a substantive and a procedural element – by referring to cyber threats to peace and security as a hypothetical, while refraining from involving the Council in the matter, the GGE exercises factual control over the agenda. Procedurally, despite (or maybe because of) the lack of any authority, the GGE offers the P5 a viable alternative to bringing their views to the public. More importantly, however, the 'cyber-UNGA' offers a venue for serious discussion of the seriousness of the cyber threat. It must be asked whether the cyber threat should be considered and addressed independently or in conjunction with other, conventional or emerging security challenges.

It is therefore worth reminding ourselves that states are trust givers of the UNSC through the UN framework (Simma, 2012, p. 775) Under Article 11 of the UN Charter, the General Assembly has the power to call the attention of the UNSC to issues of international peace and security. The UNGA is instrumental in the selection of UNSC member states. Here, in addition to geographical distribution, aspiring member states' contributions to international (cyber) peace and security could be considered. The UNGA is therefore well placed to take deeper interest in state uses of ICTs and the implications thereof to international peace and security.

Estonia might become the first state to open the cybersecurity chapter in the Security Council. After all, it is likely that the Council will conclude, like the GGE so far, that the use of ICTs is covered by international law. This would suit US interests as it would counterbalance the 'cyber-UNGA'. However, is this approach going to engage the Council or not?

An obvious way for a question concerning certain uses of ICTs to be raised in Council is a devastating cyber incident with human casualties. Such scenarios have been predicted but state practice so far indicates restraint in this respect. Alternatively, the question may be framed in terms of a lasting situation that, if continued, may endanger the maintenance of peace. Here, any state invested in the issue of national and international cybersecurity, and sufficiently independent from the leading actors, is a potential pathfinder, mediator, and thought leader. The UN Secretary-General's call for prevention and greater concern of the world's well-being deserves attention in this context.

What the Security Council has to say about the use of ICTs would, of course, depend heavily on more specific framing of the issue. The P5 could take the high road by seeking agreement (and providing assurances to the world) in the dimension of strategic cybersecurity and stability. An example could be a discussion of the role of ICTs in nuclear security and a commitment to prevent the uses of ICTs in ways that would make possible inadvertent or deliberate use of the nuclear weapons.

Concluding thoughts

Any change starts with a vision for an alternative. Coming up with that vision requires a candid assessment of the current affairs – what, if anything, is wrong in state use of ICT? How can it be changed towards what is commonly seen as a viable and good alternative? What role can individual states, the Council and the P5 play in enabling, facilitating or actuating this? These questions need answers before any reforms or agendas can be credibly tabled. Fassbender's observation of there being an agreement that the SC must be adapted to the present conditions of international life begs the question what those conditions are and what is there to be adapted. Individual states, NGOs, academia, and the private sector can offer views on what constitutes the cyber portion of international contestation, how to prevent cyber conflict and how best to mitigate incidents.

The challenge of escaping being famous for being (still) alive and reflecting how much, in fact, world affairs circle around five sovereign states, has nothing to do with cyber, as is the case with most of the contestation and conflict in today's world. More than anything, the Security Council is testament to the international community living a relatively comfortable life, while rogue actors and muscle states operate just shy of the thresholds for the use of force. The P5 need to realize that their actions and inactions do not set precedents just for the periphery but also for the international community they are part of. However, without a critical mass of international effort and determination, there will not be enough pressure in cybersecurity issue circles to make a decisive turn from threat narratives to systemic risk management, governance, and stewardship.

References

Anon. (2019) Private conversations with high officials of the Russian Federation.

Council of Foreign Relations (2019) Cyber Operations Tracker. Available from: www.cfr.org/interactive/cyber-operations [accessed 27 June 2019].

von Einsiedel, S, Malone, D.M., and Stagno Ugarte, B. (eds) (2015) *The UN Security Council in the 21st Century*. Lynne Rienner, Boulder.

Fassbender, B. (2012) The Security Council. In Cassese, A. *Realizing Utopia: The Future of International Law*. Oxford University Press, Oxford.

Jones, B. (2016) The Security Council and the changing distribution of power. In von Einsiedel, S., Malone D., & Stagno Ugarte, B. (eds) (2016) *The Security Council in the 21st Century*. Lynne Rienner, London.

Kaljulaid, K. (2018) Address by the President of the Republic of Estonia Kersti Kaljulaid at the 73rd United Nations General Assembly. Available from: www.president.ee/en/official-duties/speeches/14577-address-by-the-president-of-the-republic-of-estonia-kersti-kaljulaid-at-the-73rd-united-nations-general-assembly/index.html [accessed 28 June 2019].

Krutskihk, A. (2018 and 2019). Speeches at the International Information Security Research Consortium conference. Garmisch-Partenkirchen (April 2018 and 2019) and Moscow (December 2018).

Mancini, F. (2016) Promoting democracy. In von Einsiedel, S., Malone D., & Stagno Ugarte, B. (eds) (2016) *The Security Council in the 21st Century*. Lynne Rienner, London.

Maness, R.C., Valeriano, B. & Jensen, B. (2019) The dyadic cyber incident and dispute data version 1.5. Available from: https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset [accessed 27 June 2019].

Nye, J.S. (2018) Normative restraints on cyber conflict. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Schia, N.N. (2017) Horseshoe and Catwalk: Power, Complexity and Consensus-Making in the United Nations Security Council. In Niezen, R. and Sapignoli, M. *Palaces of Hope – The Anthropology of Global Organizations*. Cambridge University Press, Cambridge.

Schia, N.N. (2018) *Franchised States and the Bureaucracy of Peace*. Palgrave Macmillan, London.

Serna Galvan, M.L. de la (2011) Interpretation of article 39 of the UN Charter (Threat to the peace) by the Security Council. *Anuario Mexicano de Derecho Internacional*, XI, 147–185.

Simma, B. (2012) *The Charter of the United Nations: A Commentary*. Oxford University Press, Oxford

Stoltenberg, J. (2019) Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London. (May 23) Available from: www.nato.int/cps/en/natohq/opinions_166039.htm [accessed 23 August 2019].

Taylor, R.H. (1988) What are these things called "operations short of war"? *Military Review*. 68.

Tikk, E. & Kerttunen, M. (2018) Parabasis: Cyber diplomacy in stalemate. Norsk Utenrikspolitisk Institutt (NUPI). Available from: www.nupi.no/en/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate [accessed 27 June 2019].

UNIDIR (2017) *The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century.* UNIDIR Resources.

United Nations (1945). *The Charter of the United Nations.*

United Nations General Assembly (UNGA) (2016) Developments in the Field of Information and Telecommunications in the Context of International Security (9 December) A/RES/71/28.

United Nations General Assembly (UNGA) (2010) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/65/201 (30 July)

United Nations General Assembly (UNGA) (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/68/98 (24 June)

United Nations General Assembly (UNGA) (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/70/174 (22 July)

United Nations General Assembly (UNGA) (2018) *Developments in the Field of Information and Telecommunications in the Context of International Security.* A/RES/73/27 (11 December)

United Nations General Assembly (UNGA) (2019) *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* A/RES/73/266 (2 January)

United Nations Secretary-General (2017) Secretary-General's Address to the General Assembly (December 17). Available from: www.un.org/sg/en/content/sg/statement/2017-09-19/secretary-generals-address-general-assembly [accessed 23 August 2019].

United Nations Security Council (1994)Resolution 960 (29 January) S/RES/960

United Nations Security Council (1994) Resolution 948 (15 October) S/RES/948

United Nations Security Council (1996)Resolution 1040 (21 November) S/RES/960

United Nations Security Council (1998)Resolution 1212 (26 November) S/RES/1212

United Nations Security Council (1999) Resolution 1267 (15 October) S/RES/1267

United Nations Security Council (2001)Resolution 1373 (28 September) S/RES/1373

United Nations Security Council (2004) Resolution 1540 (28 April) S/RES/1540

United Nations Security Council (2006) Resolution 2150 (16 April) S/RES/2150

United Nations Security Council (2006) Resolution 1738 (23 December) S/RES/1738

United States of America (1996), FM 100-20 Military operations in low intensity conflict. Available from: www.bits.de [accessed 27 June 2019].

What's in Blue (2016) Open Arria-formula Meeting on Cybersecurity. Available from: www.whatsinblue.org/2016/11/open-arria-formula-meeting-on-cybersecurity.php [accessed 27 June 2019].

Wuthnow, J. (2012) *Chinese Diplomacy and the UN Security Council: Beyond the Veto.* Routledge, London.