RESEARCH IN FOCUS

Cyber Operations and Inter-State Competition and Conflict: The Persisting Value of Preventive Diplomacy

Camino Kavanagh and Paul Cornish
September 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Acknowledgments

The authors extend their thanks to the Swiss Federal Department of Foreign Affairs for supporting the work that led to this report and to the European Union Institute for Security Studies for accepting the report for publication. The authors also wish to thank many colleagues for their reviews, anonymous and otherwise, of earlier versions of the report. Our thanks are due in particular to the following for their participation in the initial workshop and for the expert and constructive advice so generously given in the course of the project and the preparation of the report:

Gary Brown, National Defense University, Washington, D.C.; Madeline Carr, University College London; Laura Crespo and Qendresa Hoxha, Swiss FDFA; Martha Finnemore, George Washington University; Enrico Formica, Mediation Support Unit, UN Department of Political and Peacebuilding Affairs; Gillian Goh, UN Office for Disarmament Affairs; Andrew Hadley, Centre for Humanitarian Dialogue; Sean Kane, Mediation Support Unit, UN Department of Political and Peacebuilding Affairs; John Mallery, MIT; Paul Meyer, Simon Fraser University; and Patryk Pawlak, EUISS.

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Abstract

How prepared are we to manage inter-state competition and conflict in the information era? While we struggle to understand the evolving character of conflict, it is sobering to consider that the technological advances of recent decades might prove to have been triggers for a much faster-moving and more disruptive phase of human history - a phase we are only just entering. The pace and scope of technological change might become exponential, complicating our understanding and management of conflict dynamics by several orders of magnitude. If we are interested in preventing and resolving contemporary conflicts, then it is reasonable to ask whether the principles and practices of preventive diplomacy and conflict management, developed over the past 75 years, might be effective in this evolving technologically-dependent environment. They might be, but it will not be enough simply to declare that prevention is important and to insist that the relevant UN Charter provisions must apply. The principles, ideas, and mechanisms of preventive diplomacy will not survive in the digital environment of the 21st century without intelligent reassessment and very careful nurturing. States need to take a range of complementary steps - technological, normative, political, institutional - in order for prevention to take root.

Key points

- Preventive diplomacy is as valid now as in the past, even if the international environment may currently appear unconducive to its application.
- Preventive diplomacy has always been contingent upon a reasonably settled understanding of conflict and a number of critical factors. These factors include the **means and methods**, **the effects os which might trigger or escalate conflict**; **time-spatial elements** influencing how these means and methods are used; the **actors** involved; the **normative framework** against which these uses and their effects are assessed; and the **impact on civilians**.
- Cyber operations and capabilities play an increasingly central role in contemporary inter-state relations. They reflect additional **means and methods** used by states outside and within the context of armed conflict to achieve concrete operational or tactical goals within broader geopolitical and strategic objectives. Any preventive effort would need to be closely linked to diplomatic efforts dealing with the broader competition or conflict dynamics within which cyber operations or capabilities are being deployed, not just to the immediate effects of the operation per se.
- Preventive action can include early warning, fact-finding, negotiation, mediation and dialogue facilitation. It also includes applying existing rules and principles of international law, identifying if new norms - whether binding or non-binding - are needed, and establishing mechanisms to build and sustain confidence among states and between states and other relevant actors. These elements of preventive diplomacy are strong and familiar, as are the consequences of not using them when most needed.
- Cyberspace is often described as the 'wild west', a 'frontier zone', or an 'ungoverned space'. If these descriptions were accurate then the idea of exercising preventive diplomacy in contemporary inter-state relations would seem to be little more than a far-distant aspiration.
- Fortunately, these descriptions do not hold; cyberspace is neither the digital version of a 'failed state' in which no law applies, nor is it *terra nullius* (available for acquisition by expansionist or predatory powers). Similarly, a states' decision to develop and deploy cyber operations is governed by established rules, principles, practices and customs of international law and inter-state relations. These factors continue to enable the application of preventive diplomacy regardless of the means and methods used by states, whether in peacetime or in conflict.

> At the present time of heightened tensions and new threats and anxieties, there is no alternative but to return to the foundations of the global system of collective security and to uphold the purposes, principles, and central mandates of the Charter, especially as they relate to its overarching goal of prevention[1].

1 Introduction

This working paper examines the principles and practices of preventive diplomacy in relation to contemporary inter-state relations in which cyber operations and capabilities play an increasingly central role. The working paper does not regard such cyber activity as the root source of tensions between states, but rather as an additional means used by states, including though proxies, to achieve concrete operational or tactical goals that, in turn, aim to meet broader geopolitical and strategic objectives.2 We acknowledge that the effects of these uses can, however, be destabilising, and can be potentially escalatory, especially when tensions between states already exist. They can also contribute to the spread of disruption, destruction, and by extension, human suffering in the context of an existing armed conflict, in addition to rendering these conflicts more complex and protracted. Preventive efforts thus need to be deployed and assessed within this context.

The general principles and practices of preventive diplomacy are as valid now as in the past, even if the international environment may currently appear unconducive to their application.

The development of **preventive diplomacy as a discrete set of ideas and practices** has always been contingent upon a reasonably settled understanding of conflict and a number of critical factors. These factors include the means and methods, the effects of which might trigger or escalate tensions; time-spatial elements influencing how these means and methods are used; the actors involved; the normative framework against which these uses and their effects are assessed; and the impact on civilians.[3] We therefore suggest that a first step in understanding the relevance of preventive diplomacy to inter-state competition and conflict involving ICT today requires a deeper understanding of these factors.

It is not yet possible to identify a distinct and coherent set of preventive diplomacy activities that could be understood and generally acknowledged as effective in this sphere. However, it is nevertheless clear that the general principles and practices of preventive diplomacy are as valid now as in the past, even if the international environment may currently appear unconducive to their application. Furthermore, it is possible to show that there is a convincing case for such activities among a number of states, that the conditions exist for such activities, and that there is interest in, and potential for, developing more refined and effective approaches to what might in time be recognised as a discrete sub-school of preventive diplomacy. In that regard, this working paper is best understood both as a scoping study and as a baseline for further research.

2 Preventive Diplomacy and Cyberspace

Diplomacy is an all-encompassing term for the management of international relations. It includes many functions, including official representation and communication, negotiation of treaties and agreements with other governments and international organisations, trade facilitation, and local consular services. And for as long as there has been diplomacy, it has had one other, more defining and critically important

[1] UN Secretary-General Antonio Guterres, 'State of Global Peace and Security' report, April 2020.
[2] Smeets (2018) also notes, for instance, that offensive cyber operations should not be considered in themselves, but rather with reference to both their direct and indirect effects upon conflict.
[3] This is a slight adaptation of the criteria used by Oxford University's Changing Character of Conflict Platform. https://conflictplatform.ox.ac.uk/about

function; the prevention, management, and resolution of conflict. This function - preventive diplomacy - refers specifically to a form of diplomatic action taken bilaterally, plurilaterally, or multilaterally at the earliest possible stage to "prevent the outbreak, escalation, continuation and recurrence of conflict, address the root causes of conflict and assist parties to conflict to end hostilities". It is carried out by states or international or regional organisations, although NGOs, foundations, and other actors also engage in different forms of para-diplomatic activity.

Preventive diplomacy has long captured the political, diplomatic, and public imagination. Its perceived value has grown over the past three decades, notably as the end of the Cold War opened up new possibilities for more collaborative and progressive global politics. As a feature of modern international politics, preventive diplomacy is an integral part of broader conflict prevention efforts and is applicable across the conflict spectrum.

Preventive diplomacy has its basis in the Charter of the United Nations - notably the preamble to the Charter, Article 2(3) and Chapter VI - from which other universally accepted norms and practices have emerged. Conducted in different forms and in both public and private fora, in addition to action taken by individual states, it can also include the involvement of the Security Council, the Secretary-General, envoys, and other actors to discourage the use of violence at critical moments. Preventive action can include early warning, fact-finding, negotiation, mediation, dialogue facilitation, confidence building, and crisis management. These broad principles and practices of preventive diplomacy are strong, established, and very familiar, as are the consequences of not availing of them when they are most needed.

With regard to information and communications technologies (ICTs) in the context of international security, **an emerging framework negotiated at the UN is aimed at preventing conflict between states and ensuring stability in the international system.** Despite this emerging framework, the 'fit' between 20th century preventive diplomacy and 21st century conflict is not as straightforward or automatic as might be expected. The current geopolitical landscape suggests **a shift away from an earlier, if fitful, focus on preventing conflict and ensuring greater stability in the international system towards a more competitive, reactive, and therefore potentially destabilising, outlook**. It also comes at a time when the very value of diplomacy and, by extension, its preventive function are being called into question. In this new context, the effective functioning of preventive diplomacy cannot simply be assumed; rather, we suggest its status as a practice must first be fully understood, with all its strengths and weaknesses, before it can be usefully applied to contemporary forms of inter-state competition and conflict in which information technologies play an increasingly important and destabilising role.

3 The evolving character of international conflict

Until the 1990s, the goal of preventive diplomacy was principally the prevention of misunderstandings or miscalculations that might lead to the outbreak of armed conflict *between* states and to manage and resolve any dispute or conflict arising between them. This included a broad range of diplomatic efforts aimed at preventing nuclear confrontation between the two major powers; resolving border disputes; de-escalating tensions when relations between states deteriorated; and mitigating the impacts of conflicts that did turn violent. The end of the Cold War suggested that conflict between states was no longer as likely and the preoccupation with conflict shifted to conflict *within* states, many of which had been simmering on the periphery of the Cold War. This new focus led, in turn, to the emergence of a

new set of norms and practices of preventive diplomacy to manage conflict in these specific settings.[4] Their results have been mixed as many of these conflicts have become ever more complex and protracted due not only to dynamics on the ground but also to the transnational activities of organised criminal and terrorist groups as well as the national and global elite structures that protect them; and the fact that these conflicts have also become more 'internationalised'.[5]

Troublingly, and of more relevance to this paper, significant events over the past two decades suggest that violent conflict *between* states has once again become more likely. Relentless militarisation across the globe, with accelerating investment in both existing and new weapons technologies, and strains across a number of overlapping global policy issues (including trade, migration, inequality, climate change, and public health) are posing significant risks to international peace and security and requiring greater investment in preventive efforts. However, a growing disregard for multilateralism and cooperative solutions to what are essentially global problems means that this investment in prevention has not been forthcoming.

Against this background, **our societies have become highly dependent on digital technologies. These technologies do not just create significant opportunities for preventive diplomacy** (for communication and the rapid passage of information vital to critical preventive functions, such as early warning and conflict analysis). **They also create risks** (of misuse as well as over-hasty assessment, misunderstanding and miscalculation of intentions, and misattribution). The growing reliance of states on offensive cyber operations - which we understand for the purposes of this paper as a sequence of "computer activities to disrupt, deny, degrade, and/or destroy"[6] - is weakening the already porous boundaries between peace and conflict, an unwelcome development in what seems increasingly to be a fracturing international system. While it is unlikely that these kinds of activities in and of themselves will lead to armed conflict between states (i.e. their effects will be assessed against broader conflict dynamics), their frequency and deployment in the context of growing inter-state competition should give significant grounds for concern, as should their use in the event of an actual armed conflict.

Finally, the current discourse on ICT and international security reveals a tendency to reductive bias, i.e. the simplification of a complex problem in order to make it (seem) less daunting and therefore more manageable. The language used to describe and analyse inter-state competition or the possibility of conflict involving or stemming from the use of ICT often becomes politico-military in character. This is

---

[4] These include the expansion of confidence building measures (CBMs) to cover political and social issues (as per the Vienna document), as well as the development of early warning systems and targeted funding mechanisms for rapid response, the establishment of dedicated prevention structures and the ongoing use of special envoys. More specifically for the UN, in addition to the deployment of special envoys, these new norms and practices include the establishment of Special Political Missions, Peace Operations or Regional Offices; Rapidly Deployable Mediation Expertise; Electoral Assistance; Deployable Political and Human Rights Capacity; Sanctions Monitoring Groups. See: Helsinki Final Act (second and third dimensions); the Report of the UN Secretary-General. 'Preventive Diplomacy: Delivering on Results'; and 'United Nations Conflict Prevention and Preventive Diplomacy in Action: An Overview of the role, approach and tools of the United Nations in preventing violent conflict'.

[5] Kane (2020) discusses the increase in external military interventions in civil conflicts and implications for peacemaking in Kane, S.W (2020). 'Making Peace When the Whole World Has Come to Fight: The Mediation of Internationalized Civil Wars'. *International Peacekeeping*.

[6] See Smeets, M. (2018), 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly*'. Fall 2018.

Buchanan (2020) uses the 'kill chain' idea to conceptualise cyber operations - i.e. "the sequence of steps hackers cycle through in order to achieve their aims".

Some experts include state-backed espionage activity in their definition of offensive operations, particularly when it can have destabilising consequences. Additionally, in the current debate over whether sovereignty is a principle or a rule of international law, Roguski notes two interpretations of the 'sovereignty-as-a-rule approach': the *de minimis* approach and the penetration-based approach. Under the latter every penetration of computer networks located within the territory of a state is viewed as a violation that state's sovereignty (France, for instance). Roguski questions whether such an interpretation of the sovereignty-as-a-rule approach would apply to cyber espionage operations that penetrate targeted computer systems. Such a view, he notes, would run counter to the predominant view that intelligence collection, including by cybermeans, is not *per se,* regulated by international law. Roguski (2020), (pp. 4-6).

not necessarily to take issue with the military association, but to say that the military role is far from sufficient to the solution of these complex problems and that, more generally, the reductive bias can distort and narrow the environment in which we expect preventive diplomacy to operate. This is all the more relevant when considering the fact that, so far, it has been intelligence agencies or their proxies (rather than militaries) that have been central to the conduct of many states' cyber operations. This, in turn, poses challenges for preventive efforts and the normative basis underpinning them. The choice of language and terms of reference also matters. Cold War-derived language such as 'arms control', 'confidence building measures' (CBMs), and 'deterrence', for example, can have a place in the language, of course, but these Cold War-vintage terms do not, by right, occupy that place; they must be adapted and rearticulated to meet very new circumstances.

4 Means and methods

Although a number of studies use the terms 'cyber weapons' and 'cyber warfare' when referring to the technological means and methods used by states to advance foreign policy or national security interests, we have refrained from using the terms since they are misleading for our purposes, particularly from a normative perspective. Instead, we use the terms 'cyber capabilities' or 'operations', which better reflect their use both within and beyond the context of armed conflict and provide a better normative base for focusing on the actual uses and users of the capabilities, rather than the technologies ('weapons') *per se*.

“

For some analysts, cyber operations constitute a form of conflict prevention in their own right, or at minimum, a form of restraint, since the very medium through which they are deployed compels actors to cooperate in order to compete.

The emphasis on cyber capabilities or cyber operations requires some explanation and qualification, not least because **it is the capacity for offensive action that is perceived as having the most potential for destabilisation, therefore making it the clearest target for preventive diplomatic activity.**

First, it should be borne in mind that for some analysts, cyber operations constitute a form of conflict prevention in their own right, or at minimum, a form of restraint, since the very medium through which they are deployed compels actors to cooperate in order to compete. Hence, the argument goes, while 'cyberconflict' is "bounded vertically", it remains "unbounded horizontally in the potential for creative exploitation".[7] This view would explain the absence, to date, of the "most feared scenarios" and the restraint shown in well-documented disruptive activity, such as Stuxnet and the disruption of Ukraine's electrical grid. It could also be argued that it explains why, despite the warnings of pending catastrophe, including during Covid-19, the world continues to hedge risk and heavily invest in digital goods and services.[8] This view may fall short, however, in that the effects of the kind of creative exploitation referred to here - particularly when persistent - are increasingly viewed as activity that could be considered as pushing existing normative thresholds of what is or is not acceptable behaviour by states.

[7] Lindsay, J.R. (2017), "Restrained by design: the political economy of cybersecurity", Digital Policy, Regulation and Governance, Vol. 19 No. 6, pp. 493-514. Lindsay synthesises his argument noting that Cyber conflict is restrained by the collective sociotechnical constitution of cyberspace, where actors must cooperate to compete. In this regard, the "[m]aintenance of common protocols and open access is a condition for the possibility of attack, and successful deceptive exploitation of these connections becomes more difficult in politically sensitive situations as defence and deterrence become more feasible. The distribution of cyberconflict is, thus, bounded vertically in severity but unbounded horizontally in the potential for creative exploitation.

[8] Ibid.

“

Others argue that cyber campaigns or operations can reduce the harmful impact of conventional conflict on civilian populations.

Others argue that cyber campaigns or operations can reduce the harmful impact of conventional conflict on civilian populations. This argument, relating to improved accuracy and reduced collateral effects, may prove to be problematic, however, as it ignores the lessons of the recent past in terms of over-reliance on technology.[9] It also assumes that all cyber capabilities are developed and deployed under the same conditions, and that the effects of any given cyber operation, including automated cyber operations, can be contained. Moreover, this argument assumes that the target of the operation will perceive the intent of the operation with the same mindset and obviates the possibility, if not the probability, of reciprocal action on the part of the targeted state, particularly if the operations in question are persistent.

Developing and deploying cyber operations often requires significant resources: For instance, putting together an actual cyber operation like Stuxnet, the Ukraine blackout, or NotPetya - operations that are often discussed, perhaps exaggeratedly, as 'game-changers' - involve significant investment to penetrate and survey a competitor's infrastructure and networks (including cross-domain intelligence) and control-test the capabilities in question. Many offensive operations also involve seeking out and exploiting software vulnerabilities, zero-days in particular, which are and likely will remain "a key part of advanced modern cyber operations".[10] In the longer term, zero-day use can be more damaging to the state in question, as well as the entire ecosystem, although sometimes they may be used for important defensive purposes.[11] The handling of the 'eternal blue' vulnerability is a case in point.[12] And as is now well known, once out in the open, these same vulnerabilities can be reverse engineered and reused by less capable and resource rich states or non-state actors for their own purposes.

We also know that regardless of whether the involvement of a given state is suspected in a cyber operation, 'plausible deniability' is still all too easy. Indeed, despite important developments, demonstrating state involvement in cyber operations, including when proxies are used, in any diplomatically suitable, legally convincing, or politically actionable way remains difficult and highly contested. Reliance on traditional tools of preventive diplomacy such as back-channelling, negotiation, mediation, and dialogue facilitation, which by their very nature rely on knowing who the parties to an actual or potential conflict are, can be confounded by attribution challenges. **These attribution challenges are hardly very different, however, to potential escalatory events in the non-cyber realm** and a number of preventive functions can be discerned. For instance, from a technical perspective, providing evidence of state-backed activity could be compromising for the accusing state. Publication of that evidence might also serve as a deterrent in that it can reveal the means and methods or the sequence of steps used by the attacker, thus rendering them useless for future operations. Publication of technical evidence of state-backed activity can also serve an important signalling purpose,

[9] Such assertions regarding technology and collateral damage have generally tended to be deaf to history and blind to politics and to territorial realities. See for instance, Freedman, L (2013), Strategy: A History. Oxford University Press.

[10] Buchanan (2020) reminds us that hackers who are capable of finding and exploiting vulnerabilities, and moreover, "stringing zero days together in exploit chains" for even greater success "will maintain more freedom of action and offensive capability". Buchanan, B., 'A National Security Research Agenda for Cybersecurity and Artificial Intelligence'. CSET Issue Brief , Center for Security and Emerging Technology. May 2020.

[11] Ibid. (p. 7)

[12] A. Greenberg, (2018). 'The Untold Story of Non-Petya, the Most Devastating Cyberattack in History'. Wired. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/;
Kavanagh, C., (2019), 'Stemming the Exploitation of ICT Threats and Vulnerabilities: An Overview of Current Trends, Enabling Dynamics and Private Sector Responses. UNIDIR. To date only a handful of states have put in place mechanisms to vet vulnerability handling by state security agencies or to coordinate vulnerability disclosure.

another vital function of preventive action, even if often discussed using the vocabulary of deterrence.[13] From a legal perspective, it is important to recognise the persisting challenges of 'unsettled general international rules on evidence'.[14] Yet, the very absence of clear legal standards for attributing a cyberattack might actually provide a much-needed opportunity for further dialogue to clarify these 'unsettled general international rules' and reduce tensions between states. Pushing the bar to explore complementary institutional structures - both centralised and decentralised - to support attribution can also have a preventive effect.[15]

It is hardly the case that these kinds of operations would be one-off events though, hence consideration of the broader context and analysis of technical, political, and behavioural variables will likely provide a clearer indication of the actors involved, allowing for an assessment of whether third-party engagement is possible or even desirable.[16] Conversely, not every state or organisation has the resources and capacities required to gather the political and technical information (or intelligence) to inform such an assessment.

Any discussion on means and methods requires some discussion of time-spatial elements, since these, too, will influence preventive efforts. The multi-layered computer networks and systems - as well as the disparate information distribution or delivery technologies and systems that enable them and facilitate data flow are generally referred to today as 'cyberspace', or in UN circles, 'the ICT environment'. This technological 'substrate' of modern societies is made up of several interconnected layers: physical, syntactic, semantic, and pragmatic, with the first exploiting the more intangible electro-magnetic spectrum rather than physical space.[17] These physical and pragmatic layers are subject to certain sovereign governmental jurisdiction and controls.[18] The degree of jurisdiction and control depends on another slew of factors, including the boundaries of international law, the nature of a given regime, national security, economic, industry, societal, cultural, and ideological factors, as well as interests and perceptions of agency (of self and other), in terms of the capacity and condition of exerting power.

Operations can be conducted across the different layers that constitute cyberspace, simultaneously and across several jurisdictions, directly or indirectly, including through the use of proxies. Their effects might be contained within these layers; they may also be physical and can have triggering consequences within the context of existing tensions or an existing conflict involving states or non-state actors acting on their behalf. It is often assumed that cyber operations are conducted at the speed of light. Yet most operations require a degree of planning as well as an important injection of capital and capacity. And even if their effects could be immediate, it is not always the case that immediacy is desirable. Indeed, as in the real world, an operation might have various phases, punctuated by tactical moves undertaken covertly or discernibly in both the physical and cyber realms. Unlike the

---

[13] See Cornish, P. 'Digital Détente: Designing a Strategic Response to Cyber Espionage', Public Interest Report (Washington, D.C.: Federation of American Scientists, September 2012); Hollis and Finnemore argue that accusing another state of being responsible for a cyber operation serves a number of functions or purposes. These include deterrence, defence, norm/law enforcement and norm/law constitution. Finnemore, Martha and Hollis, Duncan B., 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (March 6, 2019). European Journal of International Law (forthcoming 2020); Temple University Legal Studies Research Paper No. 2019-14. Available at SSRN: https://ssrn.com/abstract=3347958

[14] See Eichensehr, K., 'The Law & Politics of Cyberattack Attribution' (September 15, 2019). UCLA Law Review, Vol. 67, (2020, Forthcoming); UCLA School of Law, Public Law Research Paper No. 19-36. Available at SSRN: https://ssrn.com/abstract=3453804

[15] Ibid.

[16] On attribution indicators, see, for example, Roguski, P. (2020), 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views. 2020 Policy Brief, The Hague Programme for Cyber Norms. (p. 16)

[17] The *physical layer* includes the physical devices that make up this layer - computers, servers, routers, networks, grids, communications channels (wires, fibre optic cables, radio, satellite) - and segments of which use portions of the electromagnetic spectrum (EMS). (Figure 1 rivileged sovereignty, notably how to sovereign governmental jurisdiction and controls. enna peace negotiations. n im

[18] Nye, J. S. (2014), The Regime Complex for Managing Global Cyber Activities. CIGI. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

physical realm, however, it is more difficult to discern whether a breach conducted, say, for espionage purposes will also serve more nefarious cyber activity downstream. From a defensive posture, this, in turn, may drive state agencies to err on the side of caution and view all intrusions as a prelude to an attack. Importantly, these different attributes complicate early warning, a critical function of preventive diplomacy.

The current emphasis on offensive operations shadows important developments in the area of cyberdefence that could carry important preventive value.

At the same time, the current emphasis on offensive operations shadows important developments in the area of cyberdefence that could carry important preventive value. For instance, while machine learning can enhance opportunities for vulnerability discovery and exploitation, it can also enhance detection, which remains "the single biggest challenge for network defenders" and, by extension, interdiction and attribution.[19] As a new research agenda posits, most major operations that have escalatory potential require time to develop and implement, thus opening a window of opportunity for detection. Advances in machine learning can offer new opportunities in this regard with the potential of "dramatically reduc[ing] the potential dangers of cyber operations" as long, however, as important challenges relating to existing applications of machine learning to cyberdefence are overcome.[20]

Preventive action in a contemporary international security context must therefore not only be **strongly attuned to the overarching [geo]political contexts, disputes, and conflicts** within which the activity is taking place. **It must be analytically competent in these other matters,** with a capacity to understand the different environments involved and the technical, normative, operational, and tactical issues that come into play across those environments. For states, this means not just developing the necessary cross-domain intelligence and capacities, but also cross-disciplinary analysis, government-wide cooperation and coordination, as well as flexible partnerships with key private sector, technical, civil society, and academic communities. For international organisations such as the UN or regional organisations such as the European Union and the Organisation for Security and Cooperation in Europe that have preventive mandates, it means broadening their scope of partners while also filling a massive cross-disciplinary analytical void to enable the kind of early warning and conflict analysis required to inform preventive action in the kinds of conflicts emerging today.[21] It also means shifting away from what has been a predominantly security-centred narrative to one that gives equal weight to other key elements of strategy, such as diplomacy and development. Some important efforts are already underway in this regard, but they will require significant investment of time and effort as well as buy-in from leadership and Member States if they are to be effective.

5 The actors

There is no consensus amongst academic, private sector, or government experts **regarding the number of countries possessing the capacity to conduct offensive cyber operations.** Estimates range **from 30 to 50**, although the methodologies used to arrive at such estimates are somewhat shaky. It is interesting to note, although perhaps not surprising, that not many states admit publicly to owning and using such capabilities. The United States and the United Kingdom were among the first to take this step. Since then, Australia, Denmark, Estonia, France, Germany, and the Netherlands have

[19] Buchanan (2020), p. 7

[20] Ibid. The research agenda notes that this would require going beyond theoretical analysis to "anchor the evaluation of machine-learning aided cyberdefence in practical and ideally measurable results".

[21] A core question that international and regional organisations need to resolve is whether these capacities should be centralised in one hub or integrated into existing thematic and regional desks.

announced or presented positions on the use of offensive cyber operations or on their views of how international law applies to said operations.[22] Some have simply conducted such operations, acknowledging responsibility after the fact.[23] Other states prefer to maintain plausible deniability, leaning on proxies or self-proclaimed patriots to conduct campaigns on their behalf. These proxies and patriots might enjoy a full range of command and control relationships with the government, ranging from direct control to passive encouragement and tolerance.[24] In yet other cases, many states deliberately choose not to reveal a cyber offensive capability for political and/or strategic reasons and choose to use other language.[25] These states might have chosen to project a deterrent effect through deliberate strategic ambiguity, a version of the so-called 'Neither Confirm Nor Deny' (NCND) doctrine developed during the Cold War, whereby states would decline to declare either their nuclear capability or the circumstances in which that capability would be used, or both.

It is not the case that only those countries mentioned above are - or could be - capable of offensive cyber activity. The ICT tools and practices necessary to conduct an effective offensive cyber operation are more or less commodities at the disposal of many states willing to invest the necessary capital and develop the necessary capacities to render them useful for espionage or military purposes - 'dual use' in Cold War parlance. There is therefore a strong argument for strengthening the transparency-accountability combination as a core element of the preventive diplomacy toolbox. States would be more forthcoming as to their capabilities and, more importantly, as to the national doctrines, policies, authorities, as well as the international law, governing the use of these capabilities. This could be done through existing regional or sub-regional platforms centred on building confidence between states, or through bilateral or plurilateral talks. For some, this might mean encouraging or promoting a 'race to the surface', as opposed to a race to the bottom, with respect to the public face that states create for their cybersecurity postures. However, there is the real risk that such a race to the surface might provoke more tensions with reciprocal action further cementing existing security dilemmas.[26] As more and more countries state their 'legitimate right' to develop and use cyber capabilities, others will want to follow suit and - as has been the case with other capabiities - may not be wedded to obligations under international law regarding their use and associated questions of transparency and accountability.

What we already know with respect to cyber capabilities and operations is that states are not the sole and often not even the principal actors in the ecosystem. There is a growing concern that soon even non-human, advanced automated or machine learning systems might, too, play a part. At present, however, criminal actors or transnational criminal organisations, violent extremists, and terrorist groups are active participants in both international and civil conflicts, often with the acquiescence of elite

---

[22] For a comparative analysis of the views of seven states (Australia, Estonia, France, Germany, the Netherlands, the United Kingdom and the United States) on the application of international law to cyber operations, see Roguski, P. (2020), 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views'. 2020 Policy Brief, The Hague Programme for Cyber Norms. (p. 16).

[23] In May 2019, Israel declared it had "thwarted an attempted cyber offensive [by Hamas] against Israeli targets". Following a 'defensive cyber operation' to knock the cell offline, the IDF proceeded to conduct an air-strike against the Hamas cyber operatives. See: Cimpanu, C., 'In a first, Israel responds to Hamas hackers with an air strike'. ZDNet, 05 May 2019. Available at: https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/; and Newman, L.H., What Israel's Strike on Hamas Hackers Means For Cyberwar'. Wired 06 May, 2019. Available at: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/ For a more recent example, see Baram, G. and Lim, K., 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks', Foreign Policy. 05 June 2020, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/

[24] Maurer, T. (2018), Cyber Mercenaries: The State, Hackers and Power. Cambridge University Press. doi: https://doi.org/10.1017/9781316422724; Dinniss, H. (2013). "Chapter 11 Participants in Conflict - Cyber Warriors, Patriotic Hackers and the Laws of War". In Chapter 11 Participants in Conflict - Cyber Warriors, Patriotic Hackers and the Laws of War. Leiden, The Netherlands: Brill | Nijhoff. doi: https://doi.org/10.1163/9789004229495_013

[25] For example, Switzerland's use of the term active cyberdefence might fall into this category. Art. 37 of the Swiss Federal Intelligence Act allows the Federal Intelligence Service to infiltrate systems and networks located abroad if they are used to attack critical infrastructures located in Switzerland.

[26] UNIDIR, "Preventing and Mitigating ICT-Related Conflict: Cyber Stability Conference 2018 Summary Report", http://unidir.org/files/publications/pdfs/preventing-and-mitigating-ict-related-conflict-cyber-stability-conference-2018-summary-report-en-724.pdf; and J. Mallery, forthcoming 2020.

> **What we already know with respect to cyber capabilities and operations is that states are not the sole and often not even the principal actors in the ecosystem.**

groups involved directly or indirectly in the conflict in question. The perceived low barrier for entry to offensive technologies has also raised yet-to-be-confirmed concerns that terrorist groups in particular may begin relying on offensive cyber operations to meet their ends. Some of these actors have not traditionally been the focus of - or engaged in - preventive diplomacy efforts and many states would likely remain reluctant to consider or include them or face other, more normative obstacles for doing so. This is particularly the case with terrorist groups or non-state actors operating on behalf of a state. While normative discussions relating to accountability of proxies in international law plod forward, law enforcement agencies, technical bodies such as CERTs and CSIRTs, and technology and cybersecurity companies play an important preventive function in tracking and responding to their activities.

At the same time, the behaviour or practices of some of these same actors can also undermine preventive action. Take, for instance, technology companies. States and other actors rely on vulnerabilities and other design flaws in commercial software or hardware to serve their political or military ends and inflict harm on others, and in the process, can harm the ecosystem itself. This will to seek out and exploit vulnerabilities, often absent any vetting process, has led to calls within the UN and by other actors for states to exercise responsibility and disclose vulnerabilities when discovered.[27] Only a handful of states have put in place processes to this effect. And if trends in research are considered, machine learning may very well increase the possibilities for discovering and exploiting vulnerabilities and "confer advantage" on those states that invest in the relevant technologies.[28]

This point raises serious questions about the roles and responsibilities of actors other than states in preventive efforts. The latter is particularly pertinent where major technology companies are concerned: not only do they wield significant power and influence over society, they also have a very significant role to play in protecting society's widening attack surface. Yet despite many efforts to overcome challenges relating, for example, to software vulnerabilities, it is not entirely evident that either companies or states are making the most effective policy and regulatory decisions. To muddy the waters further, a slew of government actions - regulatory, commercial, national security - tying many of these same global technology companies to government surveillance and intelligence gathering work, contentious defence R&D, or national positions or interests in negotiating fora makes their engagement in critical prevention activities more complicated.

Technical bodies, academics or academic groupings, research institutes, and civil society organisations are also critical to preventive efforts and may well be **critical to future cyber-related fact-finding, monitoring, or investigative mechanisms** that are, in turn, **critical to broader conflict prevention or resolution efforts**. Some have been trailblazers in calling out states on the harms posed by government use of surveillance capabilities and the potential harms or conflict potential of growing reliance on offensive cyber operations. Others have been critical in supporting para-diplomatic activity,

---

[27] For instance, the 2015 report of the UN Group of Governmental Experts called states to "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". Para. 13 (j), Developments in the field of information and telecommunications in the context of international security (UN document A/RES/70/237). The Global Commission on the Stability of Cyberspace called for States to Create Vulnerability Equity Processes. This would entail "creat[ing] procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favour of disclosure". See: https://cyberstability.org/norms/#toggle-id-5

[28] Buchanan (2020) discusses how machine learning might be used to enhance existing automated tools to help find exploitable vulnerabilities. Already existing vulnerability detecting tools - known as 'fuzzers' "provide carefully crafted inputs to computer code, seeking failures that would reveal a vulnerability. Researchers are now exploring how machine learning might improve the analysis of data generated by fuzzers and find vulnerabilities that would go unnoticed using current methods.

such as bilateral or plurilateral track 1.5 and track 2 dialogues, and in maintaining channels of dialogue amongst research and scientific communities across geopolitical and ideological divides. Whether as standalone 'cyber dialogues' or conducted within a broader strategic, political, or military dialogue, these initiatives are essential for building confidence and ensuring the appropriate mechanisms are in place in the event of a crisis and potential escalation. The current lack of movement in these processes and initiatives does not bode well for preventive efforts.

6 Normative considerations

Cyberspace is often described, if erroneously, as the 'wild west', a 'frontier zone', or an 'ungoverned space'. If these descriptions were accurate then the idea of preventive diplomacy in conflicts that have a cyber dimension would seem to be little more than a far-distant aspiration. If cyberspace really is an area in which 'anything goes', in which social *mores* and customs are not (yet) developed, and in which there are neither laws nor law enforcers, then preventive diplomacy would have none of the ideational or procedural infrastructure needed for it to operate. Fortunately, these descriptions do not hold; cyberspace is neither the digital version of an 'ungoverned space' or a 'failed state' in which no law applies, nor is it terra nullius (available for acquisition by expansionist or predatory powers), even though at times both descriptions might seem apt. Established rules, practices, and customs of inter-state relations do perform, at the very least, an enabling role for the application of preventive diplomacy in the kinds of conflicts we are witnessing today.

Cyberspace is neither the digital version of an 'ungoverned space' or a 'failed state' in which no law applies, nor is it terra nullius (available for acquisition by expansionist or predatory powers).

As noted, **to date, negotiations within the United Nations have produced a framework aimed at preventing conflict and ensuring stability and security in cyberspace.** This framework is anchored in the UN Charter and other international law (the basis of the post WWII international order); political norms of restraint and positive duties; confidence building and crisis management; as well as capacity building. In addition to serving as the basis for continued dialogue between states[29] as well as corollary para-diplomatic activity (track 1.5 and track 2 processes; confidence building; engagement with other critical actors; norm entrepreneurship on the part of non-traditional actors, etc.), these measures complement the critical work of technical bodies and standard-setting organisations. In this regard, they also play a broader, longer-term state- or institution-building role centred on resilience and cooperation both within and between states.[30]

[29] In December 2018, the General Assembly established two processes to discuss the issue of security in the use of ICTs during the period of 2019-2021, an Open-ended Working Group and a Group of Governmental Experts. See: https://www.un.org/disarmament/ict-security/

[30] Kavanagh, C. (2018), Cyberspace, the United Nations and International Peace and Security: Responding to Complexity in the 21st Century. UNIDIR. Available at: https://unidir.org/publication/united-nations-cyberspace-and-international-peace-and-security-responding-complexity

Some of the challenges relating to this initial framework as well as the process through which it was achieved are well-documented. For example, there are still significant disagreements on how key rules and principles of international law apply to the use of ICTs by states. These include questions relating to sovereignty, standards for attribution, the response framework for irresponsible behaviour, whether or not a more binding framework to restrain state behaviour might eventually be needed, and very different views on how to move multilateral discussions on responsible behaviour forward and engage other critical actors in the process. These kinds of challenges are not entirely unique to ICT-related negotiations and realities. Rather, different manifestations of the same problems exist across numerous policy agendas and can take years of dialogue and negotiation to resolve. Keeping dialogue channels open is thus critical, and this urgency is evidenced in the interest in the two new UN processes launched in 2019.

Keeping dialogue channels open is thus critical, and this urgency is evidenced in the interest in the two new UN processes launched in 2019.

Despite significant investment in the study of international law and its applicability to the use of ICTs by states over the past decade, there has been limited discussion of how traditional preventive tools, such as those outlined in Chapter VI of the UN Charter relating to the Pacific Settlement of Disputes, are applicable to state uses of ICT - even if some may already be in use.[31] Take for instance, negotiation, which is referenced alongside a number of other tools of preventive diplomacy in Article 33 (1).[32] Could track 1 negotiating processes, such as the one that resulted in the 2015 Obama-Xi agreement to refrain from IP theft for commercial purposes and establish joint incident response mechanisms, fall under this category? It certainly lowered the tone and tempo of tensions between the two powers, at least for a time.[33] What about certain components of the EU's Cyber Diplomacy Toolbox?[34] Or perhaps elements of the China-Russia cybersecurity agreement?[35] In the event of an existing armed conflict and as a means to prevent the further spread of violence, might conflict parties borrow from existing norms of restraint and confidence building measures, and apply them, for example, to peace or ceasefire negotiations?[36] Some of these norms and CBMs could be used to signal intent regarding a definitive peace settlement, serve as an early warning mechanism in the event of a violation of the settlement by cyber or other means, and, along with other measures, help build confidence in a conflict settlement process.

---

[31] See Chapter VI. Charter of the United Nations. Available at: https://www.un.org/en/sections/un-charter/chapter-vi/index.html

[32] Under Article 33 (1), Chapter VI of the Charter, "The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice".

[33] Under the agreement, the United States and China committed to refraining from conducting or knowingly supporting cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors". They also committed to establishing mechanisms for incident response. Fact Sheet: President Xi Jinping's State Visit to the United States. September 2015. Available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[34] Council Conclusions on Cyber Diplomacy. EU Cyber Direct.
Available at: https://eucyberdirect.eu/content_knowledge_hu/council-conclusions-on-cyber-diplomacy/
See also, Moret, E. and Pawlak, P., (2017), The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

[35] Pir Center (2016), 'China-Russia cyber-security pact: Should the US be concerned?
Available at: http://www.pircenter.org/media/content/files/13/14358794770.pdf; Korzak, E. (2015), 'Have Russia and China Signed a Cyber Nonaggression Pact?' The Diplomat. Available at: https://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/

[36] As discussed by Kane and Clayton (forthcoming 2020), ceasefires are a strategic component of the interactions between belligerents during armed conflict, and often the first real step between the parties towards negotiating and ending conflict as part of the broader bargaining process. Ceasefires can therefore perform various functions at different points throughout the negotiating process. They distinguish between three classes of ceasefires: cessation of hostilities, preliminary ceasefires and definitive ceasefires. Measures of restraint regarding cyber tactics and operations could be applicable across these types of ceasefires. Their application to the preliminary type would likely be more complicated however, since preliminary ceasefires generally include compliance and verification provisions.

Importantly, they could also serve important humanitarian purposes.[37] Evidently, the success of such negotiations would be complicated by numerous factors, many of which have already been highlighted in the peace treaty and ceasefire literature.[38] These include compliance and verification issues, asymmetries in power and offensive cyber capabilities of the parties, as well as the role and incentives of external actors in the conflict in question. Yet, there might still be room for creative approaches.

Then there is mediation, i.e. when a third party is called upon to resolve a dispute involving two or more parties.[39] Despite it being long regarded as an important tool of preventive diplomacy in both inter- and intra-state conflicts,[40] third-party mediation would undoubtedly be more complex in disputes or conflicts in which cyber operations are used as an enabler or force-multiplier of conventional capabilities. First, there are the time-spatial and early warning challenges discussed earlier. Additionally, since cyber operations are just one of many means that states lean on to advance their interests, **any mediation effort would need to be linked to the broader competition or conflict dynamics** within which the cyber capabilities are being deployed, including their oft multi-actor character, not just the effects of the cyber operation *per se*. Moreover, mediating these kinds of conflicts would require the consent of the parties, which normally suggests that they have reached a deadlock beyond which they cannot escalate (the somewhat disputed 'mutually hurting stalemate' theory), thus driving them to the negotiation table, or that they simply want a 'way out'.[41] This is hardly likely in relation to the kinds of cyber friction and events witnessed to date, but it could be possible in the context of efforts to bring an existing armed conflict to an end. In this regard, within the context of a broader mediation effort, a third-party mediator could raise the cyber dimension of the conflict and, drawing from existing norms, transparency, and restraint measures, provide options to the parties for consideration in their negotiations. Again, this could include refraining from certain destabilising activity - a kind of ceasefire so to speak - while broader negotiations for a definitive ceasefire and peace settlement are underway.[42] Mediators might also propose other cyber-related normative options for parties to consider as part of a lasting peace settlement.[43] A more complex situation arises, however, when a conflict includes more than two states, or, in the case of a civil conflict, is 'internationalised', i.e. it involves third parties deploying military cyber operations in support of one or several parties on the ground. Some mediators have been able to suggest additional "process design" and "substantive" elements in a mediation to end external military intervention and "shape the external strategic environment" so that it is conducive

[37] For example, parties to a conflict could specifically commit not to use cyber capabilities or operations in a manner that would undermine the provision of humanitarian assistance to war-affected populations (Clayton and Kane, 2020) or damage critical health facilities and the non-targeting of critical communications infrastructure upon which other essential public services rely.

[38] For instance, some international law scholars have discussed the waning number of peace treaties? See Bell, C. (2006). Peace Agreements: Their Nature and Legal Status. *American Journal of International Law, 100*(2), 373-412. doi:10.1017/S0002930000016705. On ceasefires, see Kane and Clayton (forthcoming 2020)

[39] Ibid.

[40] United Nations Guidance for Effective Mediation. United Nations, September 2012, https://www.google.com/search?client=safari&rls=en&q=United+Nations+Guidance+for+Effective+Mediation&ie=UTF-8&oe=UTF-8 For an overview of cases in which UN preventive diplomacy - particularly mediation and facilitation - have met success in civil conflicts, see: Nathan, L. et al (2018) 'Capturing UN Preventive Diplomacy Success: How and Why Does It Work?. Policy Paper and Case Studies. UNU-CPR

[41] This relates to Zartman's 'ripeness' concept that has been central to conflict resolution scholarship over the past three decades, even if it remains contested. Zartman, W. (2003), "Ripeness", in *Beyond Intractability*, eds. Burgess, B. and Burgess H. Boulder: University of Colorado, 2003. Cited also in Kane (2020), p. 8.

[42] Kane and Clayton (2020) lay out many of the norms that could be considered within the framework of a ceasefire negotiation.

[43] This could include norms relating to critical infrastructure protection or human rights protections including General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet.

for the peace effort on the ground.[44] Whether cyber operations merit being included or could eventually be considered within these additional elements relating to the third-party involvement in a conflict merits further exploration.

There certainly appears to be a case for deepening understanding of negotiation and mediation in relation to confrontational or adversarial situations in which cyber capabilities or operations are used and the potential of escalation is real. An important first step, however, would be to deepen and broaden the knowledge base.[45] On mediation and facilitation in particular, it would require building the capacity of actual mediators and their teams since there are few, if any, experts that combine the skills of a mediator (a very different role to that of a negotiator) and the analytical capacity (policy, normative, technical) required to navigate the digital issues that are becoming ever more central to the conflicts they are traditionally called to engage in.

Where negotiation or mediation is not desired or is not yet possible, dialogue or dialogue facilitation can be an important option. The most obvious manifestation of dialogue relating to conflict prevention and states' uses of ICTs is the different processes that have emerged within the OSCE, OAS, and ARF on CBMs. Drawing from UNGGE report recommendations on CBMs, these processes have led to agreement between participating states on region-specific transparency and cooperative measures, dialogue around which continues, albeit more meaningfully in some regions than others.[46]

The past decade has also seen a number of so-called **'cyber dialogues'**. These tend to be either standalone track 1.5 bilateral or plurilateral processes organised to advance state views on different cyber-related policy or normative issues.[47] In some instances, these dialogues are part of a broader political or strategic engagement with competitors or, in fewer instances of late, adversaries. These kinds of dialogue generally focus on thematic issues, for instance, exchanging views on how different rules and principles of international law apply to the use of ICTs by states, on exchanges of military cyber doctrine, or simply on perceived risks and threats, and often serve as CBMs in and of themselves. Few have focused specifically on identifying and exercising much-needed protocols for crisis management and de-escalation.[48] **Some of these dialogues have produced results, although their lasting effect is unclear**, fuelled in part by the absence of more in-depth study of their real or perceived value, including with regard to prevention.[49] **The freezing or postponement of many of these dialogues at present is a significant concern.**

Article 33 (1) of the UN Charter also refers to arbitration and judicial mechanisms. It is unclear, to date, how such mechanisms might be applicable to those uses of ICTs by states that present risks to the

[44] See Kane (2020). For Kane, if ending external military intervention and resettling the external environment are essential to the effective negotiation of civil wars, then mediators, too, need to learn from historical practices. Through a review of past and recent examples of multidimensional civil war peace negotiations, he suggests, cautiously, that this is already happening, including with regard to foreign troop withdrawals and other forms of military aid; and in the consideration of baseline non-interference principles to re-set the strategic external environment as was the practice in 1980s peace agreements. (pp. 21-22)

[45] This would require more inter-disciplinary study involving traditional conflict studies alongside more recent areas of study such as cyberconflict.

[46] Kavanagh, C. and Crespo, L. "Confidence Building Measures and ICT." European Foreign Affairs Review 24 (2019): 187-202; Pawlak, P., Confidence-Building Measures in Cyberspace: Current Debates and Trends' in International Cyber Norms: Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016

[47] For a general overview of Track Diplomacy, see Mapendere, J. (2006), COPOJ - Culture of Peace Online Journal, 2(1), 66-81. For track dialogues relating to cyber-related issues, see Nigel Inkster, 'Semi-Formal Diplomacy: Track 1.5 and Track 2' in P. Cornish (ed.), The Oxford Handbook of Cyber Security (Oxford University Press, forthcoming 2020).

[48] The Russian Federation and the United States signed a first agreement on these matters in 1999, leading to initial trust building and crisis management mechanisms - including the establishment of a crisis communications line - between the two powers. While the current context does not provide a strong basis upon which the two countries can effectively cooperate, these first steps to build trust between the two countries had an important influence on norms and confidence building processes at the regional and international levels. Kavanagh, C. (2018), UNIDIR.

[49] The authors will be conducting such a study on track dialogues for EUISS in the second half of 2020.

maintenance of international peace and security. Some experts have suggested that the International Court of Justice, the principal judicial organ of the United Nations established under Chapter XIV (92) of the UN Charter, would be the relevant international body for adjudicating ICT-related disputes between states. So far, however, no state has brought any such case before the court, even if some states do refer to certain ICJ judgements in explaining their positions on how certain rules and principles of international law apply to the use of ICTs by states.[50]

Article 33 (2) of the UN Charter in turn provides **a role for the UN Security Council to call upon the parties to settle their disputes by peaceful means when it deems necessary**. This can be done formally or informally.[51] Until this year, the Security Council had only addressed cyber threats through informal formats such as Arria Formula meetings, the most recent in May this year.[52] In March 2020, however, the topic was brought up under 'any other business' during a formal meeting of the Security Council to discuss a state-backed attack that had taken place several months prior.[53] Interest in the potential role of the Security Council on these issues is undoubtedly mounting, notably in light of the digital threats that have emerged around Covid-19. Yet it is unclear whether the current international environment or current Security Council dynamics are conducive for cyber threats to be included on the formal agenda, at least for the foreseeable future. From a preventive perspective, it would be unfortunate not to move in that direction.

The UN Charter also outlines **a preventive role for the UN Secretary-General.** For example, Article 98 provides that the Secretary-General, in addition to acting as such in all meetings of the General Assembly, of the Security Council, of the Economic and Social Council, and of the Trusteeship Council, shall also 'perform such other functions as are entrusted to him by these organs'. These other functions have often included functions in the field of the prevention and the peaceful settlement of disputes.[54] Article 99 notes specifically that the Secretary-General may bring to the attention of the Security Council "any matter which in his opinion may threaten the maintenance of international peace and security".[55] Drawing from the Charter and the practices of Dag Hammarskjöld and other visionary Secretaries-General, the role of the UN Secretary-General as an important peacemaking actor has evolved through extensive practice.[56]

---

[50] The European Court of Human Rights remains the only international body to have heard cyber/ICT-related cases, although, evidently, these are of a different character to the issues under study here.

[51] As noted by UNDPPA, recent years have seen increased Council engagement and flexibility in addressing emerging threats before they come on the Council's formal agenda. Through its actions, the Council can send important signals that help discourage violence and open space for preventive action including by the Secretary-General.

[52] In November 2016, the governments of Senegal and Spain organised a first Arria-formula meeting on the potential of state use of ICTs fuelling political or military tensions and the importance of the protection of ICT-dependent critical infrastructure in such cases. The government of Ukraine organised two Arria-formula meeting on the topic of "hybrid wars as a threat to international peace and security" (2017) and on the protection of critical infrastructure against terrorist attacks. (2016). C. Kavanagh (2018), 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century'. UNIDIR, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf See also What's in Blue 'Cyber Stability, Conflict Prevention and Capacity Building'. 21 May 2020. https://www.whatsinblue.org/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php#

[53] The three Council members that had called the meeting subsequently issued a statement assigning responsibility for the attacks. Joint Statement by Estonia, the United Kingdom, and the United States. March 5, 2020, https://usun.usmission.gov/joint-statement-by-estonia-the-united-kingdom-and-the-united-states-at-a-press-availability-on-russian-cyberattacks-in-georgia/

[54] The Secretary-General and Mediation. https://peacemaker.un.org/peacemaking-mandate/secretary-general

[55] Charter of the United Nations. Art. 99.

[56] The range of preventive activities has included good offices, mediation, facilitation, dialogue processes and even arbitration. In addition, the Secretary-General may take action himself or may appoint special representatives and envoys to carry out good offices and mediation on his behalf. Numerous representatives of the Secretary-General also engage in peace talks or crisis diplomacy while overseeing UN political or peacekeeping in the field, which may have mandates to help nations and regions resolve conflicts and tensions peacefully. 'The UN Secretary-General and Mediation', https://peacemaker.un.org/peacemaking-mandate/secretary-general. See also, Ramcharan, B. G., Preventive Diplomacy at the UN. Indiana University Press, 2008. Project MUSE, muse.jhu.edu/book/3994.

Most recently, these bases were conceptualised in the Sustaining Peace resolutions adopted in April 2016 by the General Assembly and Security Council, with their call for a United Nations intently focused on "preventing the outbreak, escalation, continuation and recurrence" of conflict. These resolutions refer largely to civil conflicts, however, and are silent on international conflicts. While the current Secretary-General has not yet brought any cyber-related issue to the attention of the Security Council, he has certainly identified cybersecurity as critical and cyber threats as a significant risk to the maintenance of international peace and security. The Secretary-General's High-Level Panel on Digital Cooperation laid bare the importance of stakeholder cooperation across all stakeholders for managing these threats, many of which straddle different policy areas.[57] The Secretary-General himself noted in May 2018 that in light of growing tensions between states and the increase in malicious ICT activity, he would make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious ICT activity in cyberspace.[58] The Secretary-General committed to establishing a capacity within the Secretariat to enable, *upon request*, timely support to the good offices of the Secretary-General and to provide, *upon request*, substantive expertise in support of the good offices of the Secretary-General in mitigating any conflict that may arise from cyber incidents.[59] Although it is hard to discern whether and how this specific offer might be taken up by states, it is nonetheless likely that tensions arising from or spilling over from cyber-related incidents within the context of existing or potential conflicts will require the attention of the Secretary-General. To this end, the Secretariat is seeking to bridge significant capacity gaps by developing the analytical capacity and the partnerships necessary to support the Secretary-General in these and other situations that have a bearing on the organisation's preventive mandate and practices.[60] Undoubtedly other multilateral organisations with preventive mandates will seek to develop these kinds of in-house capacities.

Finally, as the main deliberative, policymaking, and representative United Nations organ, **the General Assembly also plays an important role in calling on states to comply with their international obligations to prevent conflict or to bring situations of concern to the attention of the Security Council.**[61] Where state uses of ICTs are concerned, the normative work that has been undertaken by the General Assembly's First Committee on International Security and Disarmament, its Groups of Governmental Experts, and the Open Ended Working Group has strong preventive underpinnings.[62]

Nevertheless, these and other preventive possibilities of the UN Charter, as well as the rest of the normative framework negotiated at the UN, face important challenges: an increasingly unpredictable international order and disregard for multilateralism; growing tensions between the major powers and the groupings they support or exploit; and immense political, economic, social, and technological divides between and within states. As a result, the intended effect of the framework is under serious strain. Dialogue between the major powers is at a post-Cold War low. Meanwhile, investment and

---

[57] The Age of Digital Interdependence. Report of the High-Level Panel on Digital Cooperation. New York, 2019, https://digitalcooperation.org/news/

[58] Good offices refer to a diplomatic means for the settlement of disputes. It is one of the more modest forms of third-party engagement in a conflict or dispute. Good offices figure in the UN Security Council's repertoire of good practices and is a staple of UN Secretaries-Generals' engagement in preventive diplomacy and broader conflict prevention. See: Lapidoth R. (2006), 'Good Offices' in Max Planck Encylopedia of International Law Max Planck Encyclopedias of International Law [MPIL]. See also UN Security Council, Repertoire of Practice. https://www.un.org/securitycouncil/content/repertoire/representatives-mediators-coordinators-and-good-offices

[59] The Secretary-General's good offices can be provided - upon request - to parties in conflict through the Secretary-General's personal involvement or the dispatch of diplomatic envoys to areas of tension around the world. https://dppa.un.org/en/prevention-and-mediation.

[60] This is a global mandate but can also be country-specific. On capacity development within the UN, see the 'Digital Technologies and Armed Conflict Mediation" report and Toolkit developed jointly by UN DPPA's Mediation Support Unit and the HD Centre in 2019 and around which work continues, https://peacemaker.un.org/digitaltoolkit. UN DPPA's Policy and Mediation Division is currently engaged in a broader stream of work relating to Digital Technologies and Conflict Prevention. A core aim of both initiatives is to build internal capacity and deepen awareness of how digital technologies affect preventive mandates.

[61] See Chapter IV of the UN Charter.

[62] For an overview of this work, see: Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/ict-security/

interest in diplomacy (critical for socialising the measures recommended in this framework) is waning at the same time that investment in intelligence and surveillance capabilities is mounting and in some countries, defence expenditure - including in cyber and other technological capabilities for battlefield use - is reaching a new high. In short, **some might argue that the preventive value of this normative framework is losing valuable currency at a time when it is most urgently required.**

7 The impact on civilians

Concerns about the impact of cyber operations and other uses of ICTs by states on civilians have grown in tandem with the growth in Internet connectivity recorded each year around the world, **yet these concerns have yet to shift behaviours in any meaningful way.**

The growth in Internet connectivity and the flow of data that ensues (which some describe as a *tsunami*), might be described as revolutionary - not just technologically but also, and perhaps more significantly, in terms of politics, economics, and opportunity. There seems no end in sight, no natural limit to this expansion. If, as is often asserted, the expanding global communication infrastructure not only *shapes* but also *improves* all dimensions and all levels of human life, then it is clear why it should be so popular and why even more adoption should be encouraged and welcomed. But if the data *tsunami* represents economic, political, and individual opportunity, it is also the case that cyberspace can be a vector for challenge, insecurity, instability, inequality, crime, and competition with significant societal implications.

“

As in every other field of human interaction, cyberspace thus makes both negative and positive security demands: security is necessary not only to keep adversaries and predators at bay, but also so that the opportunities that cyberspace offers can be fully exploited.

As in every other field of human interaction, cyberspace thus makes both negative and positive security demands: security is necessary not only to keep adversaries and predators at bay, but also so that the opportunities that cyberspace offers can be fully exploited. These demands can in themselves create more insecurities, particularly for civilians.

Ironically, *tsunami* was also the name given to a 'network stress tester' software application which, in certain circumstances, could be used in a denial of service attack. For the purposes of this working paper, two challenges arise when considering the adverse effect on civilians of state misuse of cyberspace. First, intense (and growing) dependency on digital technologies (i.e. the exploitation of the opportunities they offer) is translating into increasing inequalities as well as increasing vulnerability to the activities of aggressors, predators, and so on. The 'attack surface', as it is often called, widens the more it is used and the more technologies advance. And it is precisely because of this growing dependency on digital technologies that the second challenge arises: It is increasingly difficult to expect a credible separation of ‘state’ from ‘non-state’, ‘military’ from ‘civilian’, and ‘combatant’ from ‘non-combatant’.[63] This is a very significant departure from past practice in which the possibility and the propriety of such a demarcation was largely acknowledged, even if, sadly, not always observed.

In the context of our growing dependency on digital technologies and these blurring demarcations, research institutes and civil society groups have long been warning of the impacts of state-backed cyber operations on civilians. Indeed, the potential human costs of state-backed cyber operations and other

[63] Paul Cornish, 'Cyber Deterrence' in P. Cornish (ed.), *The Oxford Handbook of Cyber Security* (Oxford University Press, forthcoming 2020).

state uses of ICTs can be significant.[64] The human rights implications are well documented. So, too, are other harms, such as social and economic harms that have consequences on peoples' livelihoods, well-being, and in many cases, their very survival.

Concerns about the human costs of cyber operations conducted as part of ongoing tensions or conflicts between states have become all the more acute during the Covid-19 pandemic.

Concerns about the human costs of cyber operations conducted as part of ongoing tensions or conflicts between states have become all the more acute during the Covid-19 pandemic. With many hospitals at their limit and mortality rates rising, the additional harm and real-life effects of bringing a hospital or emergency service offline are significant. These concerns have framed the spate of recent statements or calls for restraint regarding cyberattacks against health care facilities and critical research institutes[65] and for countries 'to exercise due diligence and take appropriate actions against actors conducting such activities from their territory'.[66]

If the effects of such operations are already palpable outside the realm of conflict, **there is no doubt that during an actual armed conflict the potential for harm and human suffering would be even more significant**. Although some states have thought about how key humanitarian principles such as distinction and proportionality apply to cyber operations, this thinking is still evolving and is not yet universally accepted. If current conventional operations in different armed conflict contexts are anything to go by, the likelihood of these principles being respected by warring parties is unfortunately limited.[67] Nonetheless, certain preventive efforts, such as ongoing dialogue on these core IHL principles, ensuring greater domestic and international transparency and accountability in how they are being considered in military and other state-backed cyber operations and tactics, remain important.

8 Concluding remarks

How prepared are our political and diplomatic institutions (national, regional, multilateral) to manage contemporary manifestations of inter-state competition and conflict and their complex cyber or technological components? What about the human factor? How can we expect age-old principles aimed at protecting civilians or norms protecting fundamental rights and freedoms to be respected with regard to cyber operations and other state uses of ICTs if we don't confront the fact that these existing norms are being constantly violated in the physical realm by states across the globe? To what extent are traditional prevention approaches compatible with deterrence approaches, notably with regard to

[64] 'The Potential Human Cost of Cyber Operations', ICRC, November 2018. https://www.icrc.org/en/document/potential-human-cost-cyber-operations

[65] Akande, D., Hollis, D. B.; Koh, H.H., and O'Brien, J., 'Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector'. 21 May 2020. Available at: https://www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/; 'World Leaders Call on Governments to Stop Cyberattacks Plaguing Healthcare Systems', Cyber Peace Institute. 26 May 2020. Available at: https://cyberpeaceinstitute.org/blog/2020-05-26-world-leaders-call-on-governments-to-stop-cyberattacks-plaguing-healthcare-systems

[66] Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic. 30 April 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

[67] See, for instance the Physicians without Borders, 'UN Investigation into Recent Attacks on Health Care in Syria is a Positive Step, But Overdue and Insufficient', or the New York Times piece, 'The U.N. Tried to Save Hospitals in Syria. It Didn't Work.' Available at: https://www.nytimes.com/2019/12/29/world/middleeast/united-nations-syria-russia.html

offensive cyber operations? How can we more effectively assess the value of cyber-related dialogues, particularly their preventive value? How can we better promote research (for instance, in artificial intelligence) that reduces, rather than enhances, the potential dangers and harms of offensive operations? How can normative and confidence building efforts relating to ICTs and international peace and security best keep pace with developments in technology that can increase or reduce the potential dangers of offensive cyber operations? What would be the most feasible way to nudge the discussion on attribution forward, particularly with regard to the normative dimension? How can multilateral organisations with important preventive mandates be most effectively strengthened to deal with the cyber components of international conflicts or civil conflicts with international dimensions? How might considerations relating to cyber operations be integrated into traditional tools of negotiation or armed conflict mediation? Will the UN Security Council exercise more responsibility on these issues? In what kinds of 'cybered'contexts might the deployment UN Secretary-General's good offices have most effect? What is the case for using existing arbitration or judicial mechanisms to resolve disputes with a strong cyber dimension? What more can be done in science diplomacy, taking the example of the Pugwash Conferences on Science and World Affairs? Is it possible for global technology companies - critical to many preventive efforts - to contribute to preventive efforts in a neutral and impartial manner?

The questions and the observations laid out in this paper highlight the complexity of the current context and they highlight that prevention, too, is complicated. Declaring that prevention is important and that the relevant Charter provisions apply is hardly enough. States need to take a range of complementary steps - technological, normative, political, institutional - in order for prevention to take root. The current moment presents an important opportunity to reassess the value of preventive diplomacy as it might apply to contemporary forms of inter-state competition and conflict and their technological components. While we struggle to understand the evolving character of conflict and to distinguish between hazard and opportunity, it is sobering to consider that the technological advances of recent decades might prove to have been triggers for a much faster-moving and more disruptive phase of human history - a phase we are only just entering, catapulted forward by the Covid-19 pandemic. The future might turn out to be anything but a comfortably linear projection from the present, a future made more or less comprehensible by trend analysis, worst-case planning, war gaming, risk assessment, scenario and contingency planning, and so on - and made manageable by the long-established practices of preventive diplomacy. Instead, the pace and scope of technological change might be on the cusp of becoming exponential, complicating our understanding and management of conflict dynamics by several orders of magnitude. If we are interested in preventing and resolving contemporary conflicts, then it seems reasonable enough to ask whether the principles of preventive diplomacy, together with the highly-evolved conflict management mechanisms and practices developed over the past 75 years, might be effective in this evolving technologically-dependent environment. They might be, but only after careful thought and consideration of their advantages and limitations; these principles, ideas, and mechanisms should not be expected to survive in the digital environment of the 21st century without intelligent reassessment and very careful nurturing.

About the authors

Dr Camino Kavanagh is a Visiting Senior fellow with the Dept. of War Studies, King's College London as well as a non-Resident Scholar with the Carnegie Endowment for International Peace. She serves on the advisory support team to the two negotiating processes underway at the United Nations on ICTs and international security (UN OEWG and UN GGE) and served as consultant/rapporteur to the 2016-2017 UN GGE. Currently senior advisor to the UN Department of Political and Peacebuilding Affairs on issues pertaining to digital technologies, mediation and conflict prevention, over the past decade she has also served as consultant to the UN Secretary-General's office in the development of his Strategy on New Technologies and worked on a range of policy initiatives relating to ICTs and international/ regional security with the OSCE, OAS, UNIDIR and national governments. Prior to this, Dr Kavanagh spent over a decade working in conflict and post-conflict settings, including with UN peacekeeping operations. Research interests include international security; digital technologies/ICT and international law, policy and history; conflict prevention and crisis management; transnational threats; national security; and cyber security.

Prof. Paul Cornish is Visiting Professor, LSE IDEAS, London School of Economics. He was educated at St Andrews, LSE and Cambridge Universities. He served in the British Army and the Foreign & Commonwealth Office and has held senior appointments in UK research institutes and universities: Chatham House; the UK Defence Academy; the Centre for Defence Studies at King's College London; RAND Europe; and the Universities of Cambridge, Bath and Exeter. His work covers international security, national strategy, arms control, the ethics of armed force, civil-military relations and cyber security. He was Co-Director of the Cyber Security Capacity Building Centre at Oxford University from 2013-18 and Professorial Fellow in Cyber Security at the National Security College, Australian National University in 2017. His most recent publication is *Interests, Ethics and Rules: Renewing UK Intervention Policy*, co-authored with Nigel Biggar, Rob Johnson and Gareth Stansfield (February 2020: www.cityforum.co.uk/). He is editor of the *Oxford Handbook of Cyber Security* and author of *Cyber Security: A Very Short Introduc*tion, both to be published by Oxford University Press in 2020 and 2021 respectively.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.