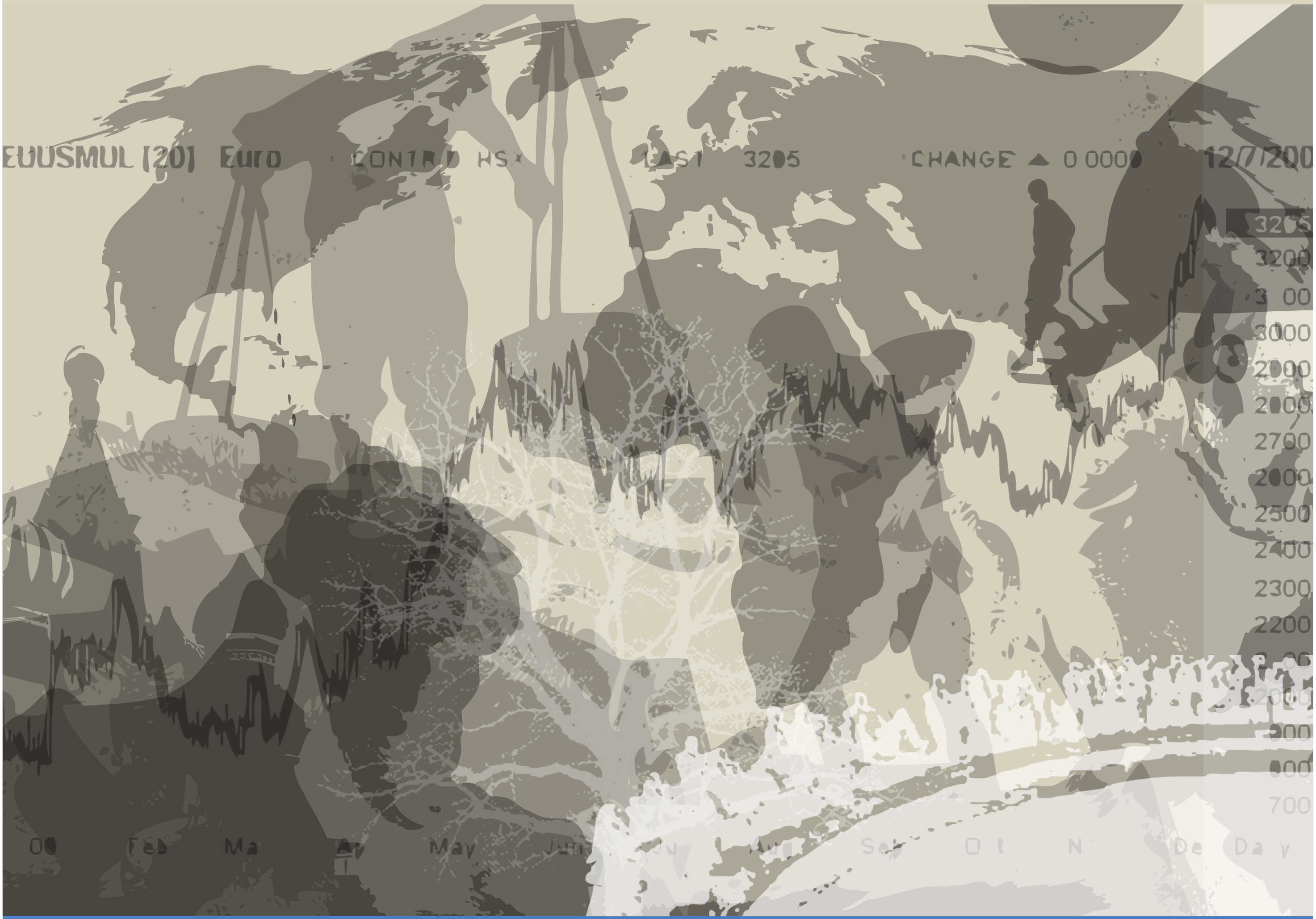
Norwegian Institute
of International
Affairs

The Politics of Stability: Cement and Change in Cyber Affairs

Mika Kerttunen & Eneken Tikk



NUPI Report
[4 / 2019]

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

Any views expressed in this publication are those of the author. They should not be interpreted as reflecting the views of the Norwegian Institute of International Affairs. The text may not be printed in part or in full without the permission of the author.

Visiting address: C.J. Hambros plass 2d
Address: PB 7024 St. Olavs Plass
0130 OSLO, Norway
Internet: www.nupi.no
E-mail: post@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

The Politics of Stability: Cement and Change in Cyber Affairs

Mika Kerttunen & Eneken Tikk

Published by the Norwegian Institute of International Affairs

Contents

Introduction

Stability is a delicate attribute of public international order. If pursued to its absolute, it could paralyse the development and progress of humankind. If marginalized, it could fuel injustice, violence and conflict.

Several differing concepts of 'stability' can be identified in international affairs. The United Nations Security Council uses the term to express a desirable state of affairs, almost synonymous with the concept of 'peace'. In a 1992 'Note by the President of the Security Council', various sources of instability were seen as threatening peace and security. The Council recognized that otherwise welcomed political changes may bring new risks to stability and security, especially stemming from changes to state structures. As the Council observed, 'non-military sources of instability in the economic, social, humanitarian and ecological fields' had become threats to peace and security.[1] Similarly, in 2005 the Council discussed the food crisis in Africa as a threat to peace, security and stability.[2]

In other contexts, the UN has identified ecological damage, disruption of family and community life as well as greater intrusion into the lives and rights of individuals as endangering stability.[3] A 2017 Security Council Resolution affirmed that regional and bilateral economic cooperation and development initiatives play a vital role in achieving stability and prosperity.[4]

Inviting states to act in ways that can generate and support long-term, sustainable peace and set new thresholds for civilization, the Security Council believes that stability can expand the margins of peace. Here the Council supports expectations of adherence to shared values and commitment to international obligations, not just regarding the actual absence of war and violence, but also in connection with sustainable societal and dignified human life. Individually, however, states may accept wider margins of insecurity between peace and conflict. Stability

[1] United Nations Security Council, Note by the President of the Security Council. S/23500 (1992).

[2] United Nations Security Council, Repertoire of the Practice of the Security Council, 2004–2007.

[3] UN Secretary-General, An Agenda for Peace. A-47-277 S-24111 (1992).

[4] United Nations Security Council, S/RES/2341 (13 February 2017).

is an always-contingent condition towards which all states aspire, using highly individual formulas for determining what needs to be stabilized, why and how. Therefore, we hold that stability is a political arrangement.

With cybersecurity now ranking high among global concerns, the international dialogue has begun to take up issues of stability in and for cyberspace. In 2010 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) first noted that, in the context of ICTs, threats and disruptive activities 'carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole'. Further, 'uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception'. Accordingly, the 2009–2010 UN GGE recommendeddialogue on measures for confidence-building, stability and risk reduction.[5] The 2012–2013 and 2014–2015 UN GGEs continued to study relevant developments, but the 2013 and 2015 reports did not explicitly examine the meaning, purpose and conditions of stability.[6]

In November 2018, the Global Commission on the Stability of Cyberspace, inaugurated one year earlier 'to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace', launched six norms pointing 'the way to new opportunities for increasing the stability of cyberspace'. However, the Commission has not examined or explained the very concept it was established to explore. Quite the contrary, the Commission argues that its proposed norms will be used to define what cyber stability actually is.[7]

Focusing on the interrelationship between international peace and stability, and ways of achieving both in the context of ICTs, we will offer a model of stability of cyberspace. We begin by examining the concepts of 'stability' and 'strategic stability' as understood with regard to international security. This conceptual analysis is followed a

[5] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201 (30 July 2010), # 1, 7, and 18. (UN GGE 2010)

[6] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98 (24 June 2013) and A/70/174 (22 July 2015) (UN GGE 2013, and UN GGE 2015, respectively).

[7] Global Commission on the Stability of Cyberspace, Norms Package Singapore (November 2018), p. 5. Available at https://cyberstability.org.

presentation of by the political claims of stability expressed in national and international cyber- and information-security discourses. Drawing on the conceptual approaches and the political claims, we then model the stability of cyberspace in three interlinked and reinforcing dimensions: 1) *equal and inclusive international relations*; 2) *prevention of war: the minimal peace*, with emphasis on averting a devastating nuclear war between the superpowers; and 3) the *functionality of global and national technical systems* and services. After discussing how international law, preventive diplomacy, confidence-building measures, and norms of responsible state behaviour can support cyberspace stability,[8] we conclude with recommendations for action aimed at helping to create and maintain a stable – resilient and adaptive – cyberspace.

[8] The UN GGEs have studied international law, confidence-building, capacity-building, and norms, rules and principles of responsible state behaviour in the context of international security. The Western states have started to group international law, voluntary norms, rules and principles of responsible state behaviour, confidence-building measures and cyber capacity-building together, as comprising an international stability framework for cyberspace.

Stability in international security

In the International Relations literature, 'stability' is not explicitly defined.[9] The term frequently refers to a desired outcome of international order and a pre-condition of peaceful international and domestic life.[10] When assessing or describing stability, scholars focus on three elements of the international system. First, they look at the *nature of the international system* – for example, as hegemonic, bipolar or multipolar. Second, they enquire into the *means* or *institutions* designed for managing power relations within the international system – for example, the balance of power, hegemony, nuclear weapons (and deterrence), collective security, world government, peacekeeping, war, international institutions, international law and diplomacy.[11] Finally, they examine the *nature of international actors* and their interactions, typically seeing democracy and trade as stabilizing factors and the basis for the internal strength of states.[12]

According to Deutsch and Singer,[13] systemic stability increases the likelihood of the (international) system retaining its essential characteristics. In a stable international system, no single nation can become dominant, while the survival of the most members (states) is ensured and there is no large-scale war. Consequently, stability, for a single state, represents the probability of its 'continued political independence and territorial integrity without any significant probability of becoming engaged in a war for survival'.[14] Hurwitz's five

[9] Several schools of IR thought have offered assumptions of and approaches to stability. Tenets of realism and structural theory have been frequent. However, our interpretations and emphasis here refer more to the politics of international information security to which we have been exposed, than to the tenets of International Law and International Relations in which we have been trained.

[10] The concepts of Pax Romana, Pax Britannica, Pax Americana as well as the doctrines of Monroe, Brezhnev, and Indira Gandhi all testify to the desirability of stable world orders.

[11]See Hedley Bull, The Anarchical Society (New York: Palgrave, 2002).

[12] Helen V. Milner, 'International Political Economy: Beyond Hegemonic Stability', Foreign Policy, No. 110, Special Edition: Frontiers of Knowledge (1998), pp. 112–123 at 112–113; and Enver Hasani, 'Reflections on weak states and other sources of international (in)stability'. Available at: http://www.bundesheer.at/pdf_pool/publikationen/hasa02.pdf.

[1313] Karl W. Deutsch and J. David Singer, 'Multipolar Power Systems and International Stability', World Politics, vol. 16, no. 3 (1964), pp. 390–406.

[14] Deutsch and Singer, at pp. 390–391.

propositions – absence of violence, governmental longevity/endurance, existence of legitimate constitutional order, absence of structural change, and multifaceted societal attributes – help to operationalize stability.[15] Dowding and Kimber's criticizing views that regard stability as *regularity* of behaviour and *normalcy* in affairs, emphasize the capacity of a political actor to prevent incidents and threatening contingencies 'from forcing its non-survival'.[16] Drawing on biology and physics in studying security and survival, Boyd stresses that closed systems inevitably develop entropy that in turn will cause a systemic change, the destruction of the old and the creation of something new.[17] Similarly, Gaddis regards controlled environments as unable to cope with the breakdown of controls – 'as they sooner or later must'; further, he holds, the assumption of stability blinds us to acknowledging, accommodating and recovering from change or disturbance.[18]

Fundamentally, therefore, stability concerns an entity's capacity to resist unavoidable threats and accommodate to inevitable changes. The latter can vary between desired, required and unanticipated transformations. This conceptual understanding acknowledges the continuity of systemic functionality as the most important objective. In this view, stability does not equate to any particular *status quo,* even if one is set as the aim or example for a discourse – especially in political speech focusing on a cemented political or world order. Although stability may align with *status quo* in some circumstances, given the inherent systemic dynamics and specific cyber-technological developments, it is important to acknowledge the likelihood and imperative of constant change. Moreover, stability in its purest form, successfully denying change, necessarily remains a temporary phenomenon, even an ahistorical illusion.

Consequently, no single trend, event, or measure is necessarily stabilizing or destabilizing. In economics, abrupt or wide fluctuations in the values of currencies or commodities may slow export or import, supply or demand, thus destabilizing the functionality of the market as well as national and individual economies.[19] While escalation of a

[15] L. Hurwitz, 'An Index of Political Stability: A Methodological Note', Comparative Political Studies, vol. 4 (1973), pp. 41–68.

[16] Keith M. Dowding and Richard Kimber, 'The Meaning and Use of "Political Stability"', European Journal of Political Research, vol. 11 (1983), pp. 229–243.

[17] John R. Boyd, 'Destruction and Creation' (1976). Available at: http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

[18] John Lewis Gaddis, On Grand Strategy (New York: Allen Lane, 2018), pp. 155–156.

[19] Thus, economic headlines may speak of, e.g., stable rice prices in one country despite fluctuations in another See, for example, The Nation (Vientiane, 4 November 2016) on rice price differences in Laos and Thailand.

confrontation might, in general, be considered destabilizing, in the nuclear deterrence literature the risk of escalation is considered to promote stability.[20] Moreover, some scholars regard the proliferation of nuclear weapons as stabilizing, others are highly destabilizing.[21] The development of national and military cyber capabilities may seem alarming. However, these developments can also be seen as strengthening national systemic resilience, the ability to accommodate technical and behavioural changes, and as supporting responsible, predictable state behaviour.

[20] See especially Tanja Ogilvy-White (ed.), On Nuclear Deterrence. The Correspondence of Sir Michael Quinlan (London: International Institute for Strategic Studies, 2011).

[21] Scott D. Sagan and Kenneth Waltz, The Spread of Nuclear Weapons. A Debate Renewed (New York: W.W. Norton, 2003).

Stability in international relations

Stability is much sought after in international affairs. Our analysis begins with the US–USSR/Russian superpower relationship where the idea of 'strategic stability' was first acknowledged. From that dense nuclear relationship, we move to recent claims concerning stability that governments have presented regarding the ICT environment. Before examining specific means of achieving stability, we look at the technical concerns of stability/instability, a highly relevant aspect in the ICT environment shared by all countries.

Strategic stability

A particular reading of stability, the concept of *strategic stability,* emerged as the United States and the Soviet Union became engaged in a nuclear arms race in the 1950s. Fears of a devastating surprise attack drew attention to vulnerabilities, and to mutual capabilities to retaliate.[22] In very twisted way, the existence of a certain degree of instability, especially accepting the risk of escalation, became seen as ensuring security – or avoidance of major war – in the nuclear era.[23]

Strategic stability functions as a pattern of thought fundamental to the theory and policy of deterrence. It has become a cornerstone of superpower relations. According to Russian academic A.G. Arbatov, strategic stability indeed refers to stability of strategic nuclear equilibrium maintained for a long period of time and despite the influence of destabilizing factors.[24] The concept is dualistic, dynamic and contextual. It operates with the desire for survival and the knowledge of vulnerability as well as change and continuity. It directs

[22] Thomas Schelling, 'Foreword', in Elbridge A. Colby and Michael S. Gerson (eds), Strategic Stability (Carlisle, PA: Strategic Studies Institute, 2013), pp. v–vi; Michael S. Gerson, 'The Origins of Strategic Stability: The United States and the Fear of Surprise Attack', in Colby & Gerson, pp. 3–12; Albert Wohlstetter, RAND P-1472 (1958), available at: http://www.rand.org/publications/classics/wohlstetter/P1472/P1472.htm; and Albert Wohlstetter, 'The Delicate Balance of Terror', Foreign Affairs, vol. 37, no. 2 (1959) pp. 211–234.

[23] Ogilvy-White (ed.) On Nuclear Deterrence.

[24] Alexei G. Arbatov, Vladimir Z. Dvorkin, Alexander A. Pikaev and Sergey K. Oznobishchev, Strategic Stability after the Cold War (Moscow: Institute of World Economy and International Relations, 2010), available at https://docplayer.net/21467197-Strategic-stability-after-the-cold-war.html.

actors to take into account their own capacities but also those of their adversary. It recognizes the need to look at technical details and objective facts but acknowledges that these will change. Strategic stability has traditionally centred on nuclear weapons, but can also have application beyond them.

In the ‘Soviet–U.S. Joint Statement on the Treaty on Strategic Offensive Arms’, issued in June 1990, at a time when one of the signatories was crumbling, the parties agreed on their mutual responsibility to enhance strategic stability. In particular, reductions in several nuclear weapons systems were designed to make a first strike less likely, which in turn was said to result in ‘greater stability and a lower risk of war’.[25] A decade later, the ‘U.S.–Russia Joint Statement Strategic Stability Cooperation Initiative’ underscored that ‘continued strengthening of global stability and international security is one of the most important tasks today’. Further, it noted the need to confront ‘new challenges to international security’ and called on other nations to join in Russo–US efforts to strengthen strategic stability.[26]

The demise of the Soviet Union and the dissolution of the Warsaw Pact did not change the understanding of strategic stability in international politics. The political, economic and military rise of the People’s Republic of China has only solidified the system centred on nuclear and strategic weapons. USA–Russia and USA–China relationships and an attitude of arms control continue to function as the main conditioning framework for questions of both the established nuclear situation and emerging security/stability questions. For example, the US Nuclear Posture Review (NPR) lists the maintenance of strategic deterrence and stability at reduced nuclear force levels as one of its goals. It goes on to note that bilateral dialogues with Russia and China on missile defence, space-related issues, conventional precision-strike capabilities, and nuclear weapons issues promote more stable and transparent strategic relationships.[27]

[25] ‘Soviet–United States Joint Statement on the Treaty on Strategic Offensive Arms’ (1 June 1990), available at https://www.bits.de/NRANEU/START/documents/Washington90.htm.

[26] ‘Joint Statement on Strategic Stability’ (4 June 2000), available at https://www.nci.org/v-w-x/wh-stratstability-jtstatement-64.html. See also, ‘Joint Statement: Strategic Stability Cooperation Initiative (6 September 2000), available at https://www.armscontrol.org/print/747.

[27] Frank A. Rose, ‘Strategic Stability in East Asia’, remarks at The Johns Hopkins–Nanjing Center for Chinese and American Studies, Nanjing, China (8 December 2014).

We argue that the Russo–US strategic relationship has continued to be determined by the mutually acknowledged ultimate value of strategic stability. Here, as for the rest of the humankind, the question is one of survival. Perversely, our continued societal and biological existence is apparently held to be a function of the survivability of the US and Russian strategic weapons and command and control systems.[28]

Stability for the ICT environment

In 1998 Russia explicitly noted the United Nations of the potential use of information technologies and weapons 'for purposes incompatible with the objectives of ensuring international security and stability'.[29] The Kremlin wanted to call attention to 'actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure'– a thinly veiled reference to US information warfare policy and doctrines and its dominant technological and military position. Further, Moscow warned of 'the destructive "effect" of information weapons, which may be comparable to that of weapons of mass destruction'. To mitigate this perceived threat, Russia put forward a draft UN General Assembly Resolution that invited discussion on this and the development of 'international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons.'[30]

In line with this emphasis on bilateral superpower relations, the information security doctrines of the Russian Federation (2001, 2008 and 2016) have called for the maintenance of strategic stability, increasingly seen as threatened by the development and use of information and communication technologies. Here information security is set as a strategic objective to serve strategic stability and 'equal strategic partnership', with the purpose of creating 'a sustainable system of conflict- free inter-state relations in the information space'.[31]

[28] See the statements in the UN First Committee in 2017, by Bangladesh (Mr Kazi, A/C.1/72/PV.21, page 11) and Indonesia (Ms. Krisnamurthi, A/C.1/72/PV.2, page 6), criticizing the whole concept of 'strategic stability'.

[29] 'Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary-General', United Nations General Assembly, A/C.1/53/3 (30 September 1998).

[30] 'Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary-General', United Nations General Assembly, A/C.1/53/3 (30 September 1998).

[31] The President of Russian Federation, Information Security Doctrine of the Russian Federation (2016), # 8e, 19 and 28. See also the Doctrines of 2000 and 2008, as well as Basic Principles for State Policy of the Russian Federation in the Feld of International Information Security to 2020 (2013).

Further, Russian information security doctrines have explicitly emphasised the importance of domestic political, economic and social stability, as well as the stability of state authority.[32]

In the UN, Russia has consistently underlined sovereignty and non-intervention and non-interference in the internal affairs of other states. The ‘Arab Spring’ and the ‘colour revolutions’ in the former Soviet republics of Georgia and Ukraine kept the Kremlin cautious of the virtues of digitalization.[33] Advanced information and communication technologies – the Internet in particular – have been regarded dangerous, albeit useful, tools of subversion, information operations and the destabilization of internal order. The *international code of conduct* launched by Russia and China together with four Central Asian partners notes that the development and application of new information and communication technologies have the potential for being ‘used for purposes that are inconsistent with the objectives of maintaining international stability and security.’ The six signatories call on nations to pledge that information and communications technologies and information and communications networks will not be used to interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability.[34]

The imperatives of national security and domestic stability and the ambition to remain a powerful strategic actor, on a par with the USA and beyond, have surfaced in Russia’s calls for digital sovereignty and emphasis of national media sphere, national segments of critical infrastructure, and a separate, national Internet, *RuNet*. The Russian *Doctrine of Information Security* included in the key objectives of ensuring ‘information security in the field of strategic stability and equal strategic partnership’ the protection of the sovereignty of the Russian Federation in information space through nationally owned and independent policy, and the development of a national system of Russian Internet segment management.[35] A separate national information system would allow maximal control over the Internet routing architecture in Russia – and the flow of information in the

[32] The President of Russian Federation, Information Security Doctrine of the Russian Federation (2000, 2008, and 2016).

[33] N.P. Romashkina and A.V. Zagorskii, Information Security Threats During Crises and Conflicts of the XXI Century (Moscow: Primakov Institute of World Economy and International Relations, 2016).

[34] UNGA ‘Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General’, A/69/723 (13 January 2015).

[35] President of Russian Federation, Information Security Doctrine of the Russian Federation (2016), # 29.

networks.[36] The aim has also been to secure Russian networks, and the confidentiality, integrity and availability of information within, from external influences and attacks.[37]

In its network policy, Moscow has been following Beijing. The 'Great Firewall of China' filters and censors Internet traffic by blocking access to certain IP addresses, hijacking certain DNS addresses to lead the inquiry to false sites, and keyword filtering aimed at preventing connection to the desired website. As stated in China's 2016 *National Cyberspace Security Strategy*, Beijing sees networks as being used to 'interfere in the internal political affairs of other countries, to attack other countries' political systems, incite social unrest, subvert other countries' regimes, as well as large-scale cyber surveillance, cyber espionage and other such activities.' Moreover, political stability is regarded as a 'precondition for national development and the happiness of the people'.[38] Kazakhstan follows its partners. Its *Concept of Information Security* divides national information security into technical and socio-political aspects. The technical aspect involves ensuring the protection of information resources, systems and infrastructure; and the socio-political aspect focuses on the protection of national information space and systems of mass information.[39]

As for the USA, the White House 2011 *International Strategy for Cyberspace* regards stability as the continuation of expected and accepted norm-guided behaviour. It implicitly refers to the nuclear realm by noting: 'in other spheres of international relations, shared understandings about acceptable behavior have enhanced stability and

[36] Mari Ristolainen, 'Should 'RuNet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West', 16th European Conference on Cyber Warfare and Security, Dublin, 29–30 June 2017. Published in Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila, GAME CHANGER. Structural transformation of cyberspace (Riihimäki: Finnish Defence Research Agency, 2017).

[37] Russia Today, 'Russia can be unplugged from World Wide Web, but it's not quite ready – co-founder of Kaspersky Lab', https://www.rt.com/russia/452660-internet-draft-law-attack/.

[38] Ministry of Foreign Affairs of the People's Republic of China, International Strategy of Cooperation on Cyberspace (2017); Zhuang Rongwen, 'Scientifically Understanding the Natural Laws of Online Communication, Striving to Boost the Level of Internet Use and Network Governance', Quishi (21 September 2018). Available from: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/.

[39] 'On the Concept of Information Security of the Republic of Kazakhstan until 2016', Degree no. 174 (14 November 2011); 'Kazakhstan's cyber shield' – a priority vector of implementation of the national security of the republic of Kazakhstan', https://articlekz.com/en/article/18494.

provided a basis for international action when corrective measures are required.' The US *International Strategy* pays great attention to the functionality of the global network, 'rooted in the technical realities of the Internet', and as a common interest.[40]

Echoing the understanding of the danger of unpredictability and surprise in international relations that guided Schelling's thinking on strategic stability,[41] the 2013 'U.S.–Russia Cooperation on Information and Communications Technology Security' spoke of the need to 'reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship'.[42]

The 2014 report of the US Department of State's International Security Advisory Board on cyber stability recognized the importance of enhancing the 'continuity of relations between nations in the face of attack or exploitation through cyber means', and defined stable cyberspace in the best neo-liberal terms as:

> *An environment where all participants, including nation-states, non-governmental organizations, commercial enterprises, and individuals, can positively and dependably enjoy the benefits of cyberspace; where there are benefits to cooperation and to avoidance of conflict, and where there are disincentives for these actors to engage in malicious cyber activity.*[43]

This report emphasizes cyber stability as fundamentally depending on transparency and the knowledge on both sides [USA and Russia] of the opponent's trigger points – actions that would lead to escalatory decisions and the deployment of more powerful capabilities, which in turn may result in full-spectrum conflict. Fostering transparency, attribution, and the political will to act are regarded as the critical

[40] The White House, Washington, DC, International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (May 2011), pp. 9, 22.

[41] Thomas C. Schelling, Surprise Attack and Disarmament (Santa Monica, CA: RAND, (1958), and The Strategy of Conflict (Cambridge, MA: Harvard University Press, 1960).

[42] The White House, 'U.S.–Russian Cooperation on Information and Communications Technology Security' (17 June 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

[43] U.S. Department of State, International Security Advisory Board, Report on␟A Framework for International Cyber Stability (2014), Appendix B. Cyber security was accordingly defined in functional terms as consisting of 'organizational actions that provide assurance of legal and reliable use of cyberspace, from hardware and software systems to operations and information (data), so that it is protected and usable in the manner expected by its originators and recipients'.

underpinnings of cyber stability as well as the geopolitical, economic, technological, and legal elements of the cyber-stability framework. To avoid unintended escalation, the Board advocates setting rigorous rules of engagement for US military and civilian organizations in responding to significant attacks using cyber means.

Following the logic of the late 1980s, US–Soviet armed forces talks and the 1989 Agreement on the Prevention of Dangerous Military Activities, Russia has been proposing military-to-military dialogue and negotiations to prevent accidental cyber conflict between the two states. Washington has not responded to this call.[44] We argue that the US reluctance to such a regime, or indeed to any other cyber treaty, stems from Washington's still-perceived position of superiority, which is not to be curbed. Both the Putin and Trump administrations are clearly not satisfied with the current state of arms-control measures: President Trump more in the nuclear domain, President Putin more in the cyber domain.

Expressing their views at the UN First Committee (Disarmament and International Security) in 2017, various countries approach stability in terms of contingent, perceived problems. Factors seen as destabilizing include the arms race, inequality, unilateralism, and the build-up and deployment of military capabilities. Their statements outline a typology of stability consisting, as expressed by the national representatives, of general, comprehensive, strategic, economic and infrastructure stability. However, there is variation in the measures preferred for reaching, maintaining or strengthening such stability.

Western states promote international stability framework in and for cyberspace. This is seen as based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence-building measures, supported by coordinated capacity-building programmes.[45] In its 2018 *National Cyber Strategy*, the USA sees stability as a function of international law and voluntary non-binding norms of responsible state behaviour in cyberspace. However, it places heavy emphasis on strength: the capacity to deter, respond to and

[44] Anatoly Streltsov and Anatoly Smirnov, 'Russian–American Cooperation in the Sphere of International Information Security: Suggestions Regarding Priority Areas', International Affairs (2017). Moreover, Streltsov and Smirnov claim that numerous other initiatives Russia has put forward 'within the framework of the U.N. aimed at a joint work to examine global aspects of strategic stability, including in cyberspace' have not been taken into account'.

[45] For statements of representatives of countries or groups of countries at the UN First Committee: Ms. Bird (Australia), A/C.1/72/PV.3, page 19; Ms. Körömi (EU), A/C.1/72/PV.19, page 16; Mr Cleobury (UK), A/C.1/72/PV.20, page 10.

entail consequences against those who do not adhere to the framework.[46]

At the UN First Committee, disarmament, arms control and non-proliferation of military capabilities are obvious measures of choice. However, some countries have brought up issues of ethics, accountability, governance and adherence to principles and rules. Table 1 summarizes the 2017 UN First Committee discussions.

	Stabilizing	Destabilizing
Disarmament, arms control, non-proliferation	• elimination of particular weapons or their uses • diminishing the role and significance of particular weapons in military and security concepts, doctrines and policies • strengthening of the multilateral mechanisms of control over weapons • verification • enhanced detection • ability to mark and trace • export controls • confidence-building measures	• arms races • developing and indoctrinating new military capabilities • increase of military expenditure by major powers • reckless and rogue behaviour of states • accumulation of personnel and military equipment • force structures and positions beyond defensive goals • weaponization of space (cyberspace, outer space) • illicit trade and traffic in weapons • collateral damage and unintended effects

[46] The White House, National Cyber Strategy of the United States of America (September 2018), pp. 20–21. See also Mika Kerttunen, 'Policy of Consequences as Seen Through Social Sciences', Temple Journal of International and Comparative Law 32:2 (Fall 2018): 71-84.

	Stabilizing	Destabilizing
General	• balanced and non-discriminatory approaches to legally binding obligations • universal compliance with rules and international agreements • new rules and norms to fit the issues in question • multilateral international cooperation • access to science and knowledge • transparency • restraint • clarity through dialogue • inclusivity • global understanding of the threat situation • shared benefits	• lack of accountability • lack of governance • ethical vacuum • flexible interpretations of legal principles • gross violations of human rights and fundamental freedoms • imbalance, inequality and sense of injustice • disparities and deep, fundamental differences • norms aimed at furthering national interests • double standards in the application of non-proliferation norms • unilateral political expediency • unilateral economic benefits • discriminatory measures

Table 1. *Stabilizing and destabilizing measures as discussed in the UN First Committee, 72th session. Authors' compilation.*

Martin Libicki of the RAND Graduate School[47] regards cyber capabilities as incapable of endangering strategic stability. His main argument is that, as the employment of cyber capabilities cannot create devastating effects, the survival of the victim state is not endangered, and the availability of its cyber capabilities and conventional or nuclear weapons can be jeopardized for only a short time. Such a situation, involving limited damage and temporary harmful effects, does not necessarily demand quick response or retaliation. However, he acknowledges that the concept and perception of cyberwar have 'created new ways to stumble into war'. This risk stems from the uneasy equation between the misperceptions of the one side, and the hypervigilance of the other: states react partially blindfolded and out of fear. Moreover, an attacker may calculate that, by a decisive and surprising cyber- or cyber-supported attack, it can gain an advantage which the victim state will be afraid of escalating further. Further, Libicki mentions that if a cyberattack does not achieve its objective, the victim state may not have an incentive to retaliate, and that is contingently stabilizing. We feel, however, that such shadow-boxing represents dangerous cyber-brinkmanship where fear, misperceptions and false assumptions not only endanger stability but also threaten peace.

Figure 1 models the stabilizing and destabilizing practices used by states when considering the development and usage of cyber capabilities. We operate with (1) two ideal types of state actors: *established* and *emerging* power actors; and (2) the assumed ability of cyber capabilities to create *better effects* or create *effects in a better way*. We use the umbrella term of 'better' to incorporate such potential attributes of cyber capabilities as speed, stealth, targetedness, precision, reversibility, and being less damaging. The characteristics of 'established' and 'emerging' refer to a state's position as a regionally or globally active security and power actor. For both types of states, cyber capabilities are relatively new tools of statecraft.

[47] Martin Libicki, Crisis and Escalation in Cyberspace (Santa Monica: RAND Corporation, 2012), pp. 123–145.

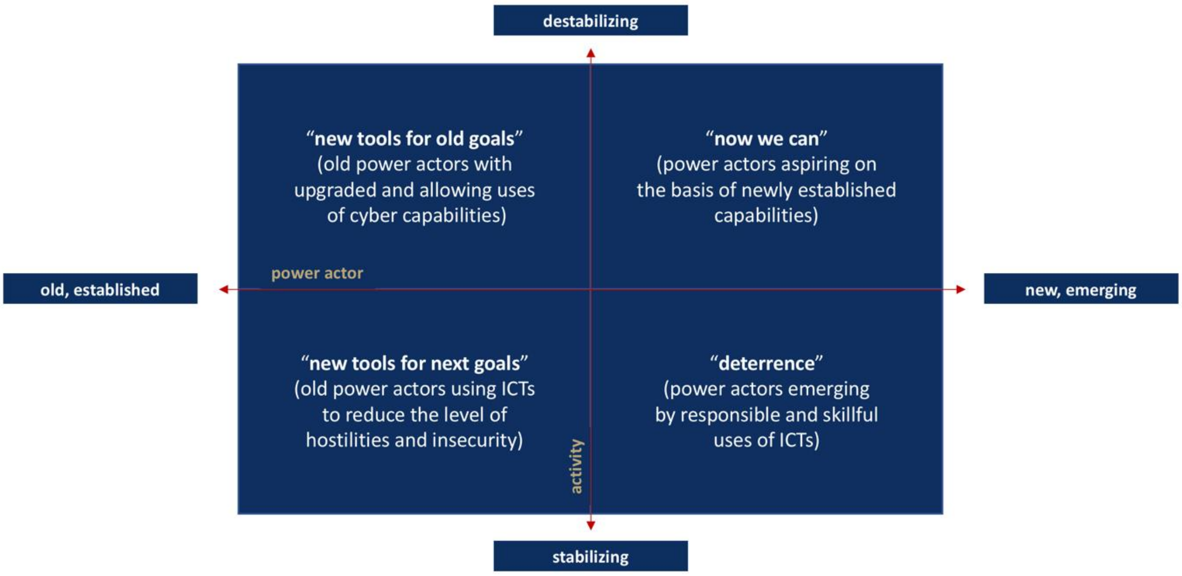

destabilizing
"new tools for old goals"
(old power actors with upgraded and allowing uses of cyber capabilities)
"now we can"
(power actors aspiring on the basis of newly established capabilities)
old, established
power actor
new, emerging
"new tools for next goals"
(old power actors using ICTs to reduce the level of hostilities and insecurity)
"deterrence"
(power actors emerging by responsible and skillful uses of ICTs)
activity
stabilizing

Figure 1. *Stabilizing and destabilizing behaviour of established and emerging power actors. Authors' compilation.*

We argue that the possession of national and military cyber capabilities does not automatically destabilize or stabilize international relations, or threaten peace, or encourage pacifying behaviour.[48] Beauty is in the eye of the beholder: our perceptions, schools of thought and political preferences determine the conclusion. However, we warn against two distinct beliefs: that cyber means, and digitalization in general, are dangerous; and that the use of cyber means in state power projection is harmless. Digitalization does improve and ease human and societal life. ICTs empower individuals and organizations. The setting where state cyber capabilities are being employed is age-old and unchanged. We are talking about human, societal, and politically conditioned environments where cognition and behaviour are uncontrollable. The first-level effects of cyber operations are not necessarily destructive, and their active use may remain undetected. However, the spill-over, second and nth-order effects and impact are unpredictable and should not be underestimated. Reckless, care-free and easy usage of cyber means may trigger latent and escalate on-going conflicts. It also leads to changes in the perceptions of normalcy and accountability.

[48] The reader is encouraged to test, question and develop this rudimentary modelling.

Stability in cyber-physical environment

ICTs have become the subject of international security dialogue as societal, economic, political and, increasingly, military functions have come to rely and depend on them. In most societies, dependence on ICTs is far greater than actual preparedness to safeguard their functions. Unsurprisingly, then, reports of cyberattacks and the development of military cyber capabilities readily give rise to angst in nations and populations.

Common to superpowers, liberal democracies and authoritarian regimes alike is the emphasis on securing essential technical national, industrial and information & communications systems in the name of stability. [49] Again, the precise objectives and preferred mechanisms will vary. Protecting of critical information infrastructure is a common area of emphasis in national cyber and information security strategies.[50] Armed forces want to protect their information, communication, command, intelligence, navigation and early warning systems. Countries with nuclear weapons are particularly concerned about the survivability and credibility of their warning, weapons and command & control systems. Technical stability is thus a factor in both political and strategic stability. Given the technological nature of the ICT environment, and the inherent vulnerability of network, systems and services to intentional and accidental disturbance, ensuring technical stability is an essential aspect of stability in cyberspace.

Should ICT infrastructure be affected by a deliberate or accidental incident, there is a logical order in which services and functions fail or are recovered (see Figure 2). Where resources to sustain online services are limited, priority will be given to critical infrastructure, services and functions. Accordingly, states have been called on to identify their critical infrastructure and services and assign responsibilities for maintaining the functioning of such infrastructure in time of crisis or emergency. Critical infrastructure and services concern assets, systems

[49] Whereas research of political stability dimensions in the ICT environment is all but non-existent, the stability of cyber-physical systems has been modestly studied. A mid-March 2019 ProQuest database inquiry using various search parameters (’cyber’, ’cyberspace’, ‘cybersecurity’, ’stability’), location of the parameter (abstracts assumed to point the core content of research; or ‘anywhere’) and the type of source (books, dissertations, thesis and conference papers) resulted in sixteen to 837 hits, mainly concerning private-sector risk-management practices.. Expanding the search to peer-reviewed scholarly journals increased the number to ca. 4600. As a point of comparison, ’cybersecurity’ without any filtering is mentioned in over 300,000 research papers of various kinds

[50] Mika Kerttunen, ‘National Cyber Security Strategies: A Commitment to Development’, Cyber Policy Institute (February 2019).

or parts thereof which are essential for the maintenance of vital societal functions, like the health, safety, security, economic and social well-being of the population; the disruption or destruction of these would be expected to have a significant impact.[51]

In 2016, the European Union added a further categorization, of infrastructure and services that require extra safeguards and protection.[52] Where the provision of a service essential for maintaining critical societal and/or economic activities depends on network and information systems and an incident would have significant disruptive effects on the provision of that service, member-states and organizations are required to make extra investments in the capacity of network and information systems to resist, at a given level of confidence, any action that would compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data, or the related services offered by, or accessible via, those network and information systems.

For stability, two further considerations are essential. Firstly, the more societal routines rely on ICTs, the more would a failure disrupt the rhythms of life. Such scenarios are generally omitted from considerations of serious international consequences or remedies, as they would concern what might be seen as a 'non-essential' function. However, if several such functions were simultaneously and/or protractedly disrupted, affecting a significant population, that would in fact constitute a serious stability challenge.

Secondly, the 'luxury' factor of ICTs should not be underestimated. The non-availability of services and applications with little or no direct value to the state affected by a cyber incident may evoke significant reactions among the populace, spurring expectations towards the authorities who may be focused on dealing with the more serious consequences of the same situation. Such 'no-access-to-Facebook' situations should be included in contingency planning, as should potential fake and deep-fake campaigns exploiting the situation.

[51] Directive 2008/114 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[52] Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, Articles 5 (2) and 4 (2).

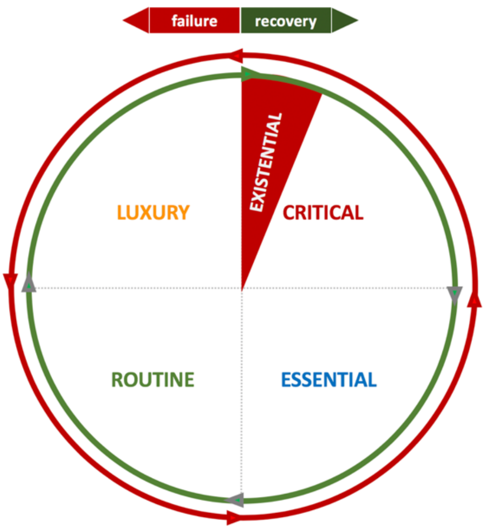


Figure 2. *Failure and recovery in relation to the relative value of systems and services. Authors' illustration.*

Applying a liberal reading to ICTs in global and domestic relations, the Obama administration's 2011 *International Strategy for Cyberspace* operationalized network stability as a condition or state in which states:

- respect the free flow of information in national network configurations,
- ensure that they do not arbitrarily interfere with internationally interconnected infrastructure
- continue to recognize the domain name system as a key technology that needs to remain secure and stable.[53]

The Trump administration has promised to offer to other governments advice 'on infrastructure deployments, innovation, risk management, policy, and standards', to further the global reach of the Internet and to ensure interoperability, security and stability.[54]

Perhaps the clearest action aimed at securing the integrity, functionality and stability of the Internet is the Dutch initiative to protect

[53] The White House, International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (May 2011).

[54] The White House, National Cyber Strategy (2018), pp. 25–26.

the public core of the Internet. [55] The initiative calls for states to exercise restraint and reserve ‘in matters of national security versus the interests of the collective Internet’ as ‘the only way to guarantee the stability of the net in the long term.’ The Dutch, however, also note that in reality, ‘those entrusted with national security are more likely to want to extend their reach than show restraint.’

The ICT environment is human-made. Thus, it is possible, to some extent at least, to insulate and isolate a country and its people from the Internet and foreign influence. In the search for stability, such 'black boxes' have been employed and are being designed. An anecdotal disagreement is attributed to Singapore’s former Prime Minister and strongman, Mr Lee Kuan Yew. For him, the American black boxes meant the ability to constantly reinvent themselves.[56]

[55] Dennis Broeders, The Public Core of the Internet: An International Agenda for Internet Governance (The Hague: The Netherlands Scientific Council for Government Policy, 2015), pp. 10, 27, 64 and 93–96.

[56] As related by Jake Sullivan, former National Security Advisor to US Vice-President Joe Biden (Jake Sullivan, ‘Yes, America Can Still Lead the World’, The Atlantic (January/February 2019).

Enhancing stability

How, then, to fulfil the tasks, or demands, of stability? In international relations and cyber affairs, various specific measures have been proposed to enhance international peace, security and/or stability.

The theory and practice of international relations offer three sets of measures for promoting stability: emphasis on the authority of international law; balance of power emphasizing the prowess of nations; and development that is attentive to justice and societal and economic factors. Power considerations, easily dated to the Melian Dialogue of Thucydides' *The History of the Peloponnesian War,* can be regarded to represent mainstream thinking. International law has been considered a European and, for the last *ca*. 120 years, also an US project that in particular China has contested its position. Developmental aspects have been promoted by market economists, aid workers, peace researchers and the UN Security Council. More radical initiatives have called for a society of states, uniformed ideology, or world government as the envisaged world order.[57]

We now turn to the UN GGE's four-tier agenda: international law; voluntary norms, rules and principles; confidence-building measures; and capacity building.[58] We also explore the potential of preventive diplomacy and resilience development.

International Law

International law follows the logic of politics.[59] Experts and scholars have noted the politicization of issues of international cybersecurity and law.[60] A celebrated consensus of the 2013 UN GGE concludes:

[57] See for example, Bull, The Anarchical Society (2002); Barry Buzan, From International to World Society (Cambridge: Cambridge University Press, 2004); Immanuel Wallerstein, World-Systems Analysis (Durham, NC: Duke University Press, 2004); and UNSC S/RES/167 (28 April 2006).

[58] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 (22 July 2015).

[59] See, e.g., Martti Koskenniemi, The Politics of International Law (Oxford: Hart, 2011); Jan Klabbers, International Law (Cambridge: Cambridge University Press, 2017).

[60] See Stefan Soesanto and Fosca D'Incau, 'The UNGGE is Dead: Time to Fall Forward' (15 August 2017),

'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[61] However, neither the GGEs that followed nor the wider international community have managed to agree on exactly how international law is to be applied.

There are several ways in which international law can be made an instrument of stability in the ICT environment. Seen through the lens of stability, unresolved disagreements about international law are less problematic than attempts to cement discrepancies in the interpretation and implementation of it. In the first instance, differences can be settled gradually through state practice, opening the particular interpretation or implementation to international reaction in a specific context. Open national positions that step back from previously acknowledged interpretation and implementation of international law, however, allow (and even call for) flexible interpretation of legal principles, thereby ruling out balanced and non-discriminatory approaches to legally binding obligations.

Both trends are evident in international cyber affairs. State activities and operations in cyberspace have led to uneasy questions about the role, even the status, of international law in preventing and mitigating state use of ICTs. States seem to be re-making their established practises.[62] To apply the stabilizing force of international law, states

http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; also Melissa Hathaway, 'When Violating the Agreement Becomes Customary Practice', in Fen Osler Hampson and Michael Sulmeyer (eds) Getting beyond Norms New Approaches to International Cyber Security Challenges (Waterloo, ON: Centre for Governance Innovation, 2017); Liis Vihul and Michael N. Schmitt, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms'(30 June 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; Robert McLaughlin and Michael N. Schmitt, 'The Need for Clarity in International Cyber Law: International Law Implications of the Lack of Consensus' (18 September 2017), https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/; Adam Segal, 'The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?' (29 June 2017), https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what); NATO CCD COE, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly', https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

[61] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98 (24 June 2013), #19.

[62] Eneken Tikk and Mika Kerttunen, Parabasis: Cyber-diplomacy in Stalemate (Oslo: Norwegian Institute of International Affairs, 2018).

wishing to uphold the rule of law ought to invoke international law in the context of cyberattacks and operations.

In parallel, states have expressed positions on how international law should be applied in cyberspace.[63] Some of these – for instance, the view that, in the context of cyberattacks, sovereignty cannot be regarded a rule of international law – diverge significantly from how international law has been understood, and applied, in international relations. In order to avoid undesirable interpretations, explicit dialogues on problematic interpretations, as well as more nuanced positions on the subject, would help to boost the stabilizing weight of international law.

Finally, certain national positions could create stability, if they promote approaches and views on international law that maximize its applicability and authority. An example is the Estonian statement from 2016:

> *For Estonia, international law is the biggest authority. We therefore strive for clarity and certainty of norms as it not only reduces the risk of intolerable practices, but provides transparency and predictability of behavior that allows us to focus on peace rather than on conflict. /…/ Let us not just suggest, but demonstrate that international law is alive, is relevant, and is useful. Let us demonstrate that we can use some of its core principles, such as good faith, and our pledge to remain bound by treaties, to modernize it to the age of smart and connected technologies.*[64]

Further exchange and views would be needed on clearly unresolved issues such as data as an object (or not) or due diligence.

[63] Some of the recent positions include the the French Cyberdefense Strategic Review, summarized on the points of international law by François Delerue and Aude Géry in France's Cyberdefense Strategic Review and International Law (https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law); UK Attorney General's remarks on the UK's position on applying international law to cyberspace, available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century;

Australia's position on how international law applies to state conduct in cyberspace (2019), available at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html.

[64] Statement by Foreign Minister Marina Kaljurand at the Conference on State Practice and the Future of International Law in Cyberspace on May 5, 2016 (https://vm.ee/en/news/statement-foreign-minister-marina-kaljurand-conference-state-practice-and-future-international).

Universal compliance with the rules and standards of international law has remained an ideal beyond reach in the current phase of the international cybersecurity process. In order to maintain and strengthen stability not all differences about international law need to be solved, however. A Faustian bargain would settle on the idea of international law, prioritizing prevention of conflict and avoiding conflict escalation, accept the employment of cyber capabilities in network intelligence, surveillance and monitoring, acknowledge the potential of cyberattacks to constitute use of force, and, in this context, focus on protection of non-combatants and civilian property.

Most alarmingly, while industrialized countries are investing in cyber military capabilities and doctrines, they remain reluctant to legally binding measures to limit such an insecurity- promoting development. The moral high ground that the West once perhaps occupied has eroded. It has also eroded international law if it is taught and received as the law of cyber operations. Perhaps the most destabilizing development from the perspective of international law itself is the side-lining of the question of binding agreements purely for political arguments, and the promotion of voluntary non-binding norms of responsible state behaviour as a substitute to the rule of law. Voluntary norms cannot provide the same amount of predictability and accountability as binding agreements do.

Norms, rules, and principles

Underlining the diversity of the views and preferred approaches, the 73rd session of the UN General Assembly in December 2018 mandated two groups to examine standards of responsible state behaviour in the ICT environment – another UN GGE (2019–2021), and an open-ended working group (2019-2020).[65]

The UN GGE's recommendations so far offer a mixed message. Firstly, the recommendations do not, in their framing or language, constitute a coherent or logical set of issues or solutions. Secondly, the issues addressed are not explicitly concerned of the questions of peace or war, conflict prevention, or the restraint of potentially escalatory behaviour, central to the continuation of peaceable relations and the functioning of

[65] UNGA, Advancing responsible State behaviour in cyberspace in the context of international security. A/RES/73/266 (December 22, 2018); UNGA, Developments in the field of information and telecommunications in the context of international security. A/RES/73/27 (December 5, 2018).

strategic and critical systems.[66] Furthermore, due to the lack of accountability deriving from their format, and the potential of diverging interpretations, the norms approach represents a step towards reduced stability. Yet, some recommendations may have stabilizing effect when implemented and (especially) when developed further.

For instance, recommendation 13(a) considers peace and security as functions of international stability and security measures.[67] This recommendation can be taken to refer to confidence-building measures, which are also examined by the Group, and to the settlement of disputes by peaceful means as specified in Articles 2(3) and 33(1) of the UN Charter.[68] Recommendation 13(b) is concerned with the challenges of attribution, state responsibility, and the prevention of conflicts and the risk of escalation during and due to a cyber incident.[69] This recommendation concerning victim-state behaviour should be complemented by a call for all states to refrain from cyberspace operations in their international relations. Such a norm would be in the spirit of the principle enshrined in Article 2(4) of the UN Charter: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.'

Recommendation 13(c), on states not knowingly allowing their territory being used for internationally wrongful acts,[70] is tightly coupled with sovereignty and the law of responsibility of states. It can be seen as constituting a new baseline for due diligence in international

[66] For a comprehensive analysis of the 2015 recommendations, see Eneken Tikk (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary (New York: UNODA, 2017).

[67] 'Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.' (UN GGE 2015, #13(a))

[68] Zine Homburger, 13(a) in Tikk (ed.), Voluntary, Non-Binding Norms (2017)

[69] 'In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.' (UN GGE 2015, #13(b))

[70] 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.' (UN GGE 2015, #13(c))

relations, state responsible behaviour and accountability to the international community.[71]

UN GGE's recommendations on the status of critical infrastructure (13(f))[72] and the authorized emergency response teams (13(k))[73] can be seen as early and very implicit attempts to establish restraint on targeting, and protection of civilian property. For international peace and stability, it is essential that these two recommendations be implemented and gain normative force. To protect civilians, non-combatants and civilian property also from the effects of the deployment of cyber capabilities, the spirit of these recommendations should be taken forward.

Regardless of the good intentions behind the UN GGE recommendations, the fact remains: the claim of voluntary non-binding norms offering predictability and stability in international relations is questionable. Responsibility, accountability and verifiably written in agreements and explicit rules create the desired effects, a predictable and stable public international order as well as conditions favourable to human and societal development.[74]

There is, however, a predominantly Russian reading of the stabilizing value of voluntarism. According to A.A. Streltsov, norms, rules and principles of responsible state behaviour will be implemented only by way of turning them into binding obligations, or as they become customary international law.[75] He highlights that the UN GGE itself has expressed hopes that the proposed norms will reflect the 'expectations of the international community' and define 'standards of responsible

[71] Liisi Adamson, 13(c) in Tikk, (ed.), Voluntary, Non-Binding Norms (2017)

[72] 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.' (UN GGE 2015, #13(f))

[73] 'States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.' (UN GGE 2015, #13(k))

[74] On the positive effect of political accountability, see e.g. Amartya Sen and Jean Drēze's research on famine, for example, A. Sen, Poverty and Famines: An Essay on Entitlement and Deprivation (Oxford: Oxford University Press, 1983).

[75] A.A. Streltsov, presentation at the Thirteenth International Forum „Partnership of States, Business and Civil Society in Providing International Information Security", Garmisch-Partenkirchen, April 22, 2019.

behaviour', the application of which will 'enable the international community to assess the actions and intentions of states'.[76]

Preventive diplomacy

In his 1992 *Agenda for Peace*, UN Secretary-General Boutros-Ghali framed 'preventive diplomacy' as covering confidence building, fact-finding, early warming and preventive employment.[77] Instead of applying this institutionally focused listing of specific measures, here we will focus on the *purpose* of preventive diplomacy. UN Charter Article 33(1) on the Pacific Settlement of Disputes provides a list of measures potentially suitable also within preventive diplomacy: negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of states' own choice. The 2001 ASEAN Regional Forum (ARF) document explains preventive diplomacy in terms of its objectives as 'consensual diplomatic and political action taken by sovereign states with the consent of all directly involved parties: [78]

- to help prevent disputes and conflicts from arising between States that could potentially pose a threat to regional peace and stability;
- to help prevent such disputes and conflicts from escalating into armed confrontation; and
- to help minimize the impact of such disputes and conflicts on the region.'

Further, the ARF lists various principles, including diplomatic, peaceful and non-coercive consultative and consensual methods and the requirement of trust, confidence, neutrality, justice and impartiality.

Basically, preventive diplomacy is linked to the existence of conflict, bringing in normative and practical difficulties to conceptualize and mitigate conflict in the ICT environment, cyberspace or in the field of

[76] Ibid, reference made to UN GGE 2015, #10.

[77] Boutros Boutros-Ghali, An Agenda for Peace: preventive diplomacy, peacemaking and peacekeeping, A/47/277 – S/24111 1992; Steven A. Zyck and Robert Muggah, 'Preventive Diplomacy and Conflict Prevention: Obstacles and Opportunities', Stability (September 2012). Available at: https://www.stabilityjournal.org/articles/10.5334/sta.ac/.

[78] ASEAN Regional Forum, 2001 ASEAN Regional Forum Concept and Principles of Preventive Diplomacy (Hanoi, 2001). See also CSCAP Study Group on Preventive Diplomacy, Chairman's Report (Yangon, 2013). Available at: http://www.cscap.org/uploads/docs/Preventive%20Diplomacy/OneOffPDMtgDec2013Myanmar.pdf.

information and telecommunications in the context of international security. Given the partial virtuality, speed and newness of the field of cyber affairs, preventive diplomacy has received the attention it deserves. The essence of preventive diplomacy lies in solving not virtual, 'cyber', issues – but the real, political ones also found on-line.

Possible measures of preventive diplomacy in a conflict with cyber dimensions could involve international teams for fact-finding; monitoring of the work of national cyber organizations (CERTs, national and military cyber-commands, military cyber-units); establishing lines and venues of diplomatic and other professional engagement or consultations; and expert teams equipped and prepared to engage in mitigation of an ongoing cyber incident, including expert teams to safeguard the function of critical national infrastructure, e.g. the power sector and telecommunications.

Confidence-building measures

Confidence-building measures (CBMs) are feature in dialogues on creating an open, accessible, secure and stable ICT environment. The 2010 UN GGE recommended 'confidence-building, stability and risk reduction measures to address the implications of State use of ICTs'.[79] The 2013 GGE report noted the how 'voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception', potentially making 'an important contribution to addressing the concerns of States over the use of ICTs by States and could be a significant step towards greater international security.' The Group recommended the following set of CBMs to promote greater transparency, predictability and cooperation:

(a) The exchange of views and information, on a voluntary basis, on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation;
(b) The creation of bilateral, regional and multilateral consultative frameworks for confidence-building;
(c) Enhanced sharing of information among states on ICT security incidents;
(d) Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums;

[79] UN GGE 2010, #18.

(e) Increased cooperation to address incidents that could affect ICT or critical infrastructures that rely upon ICT-enabled industrial control systems;

(f) Enhanced mechanisms for law enforcement cooperation, to reduce incidents that could otherwise be misinterpreted as hostile state actions.[80]

The 2015 GGE followed up by adding that CBMs can 'increase interstate cooperation, transparency, predictability and stability', and encouraged further action in the field.[81] Of the major regional organizations, the OAS and OSCE have come furthest in issuing and implementing CBMs.[82] In 2013, the USA and Russia agreed on ICT CBMs 'designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship'; measures included information exchange, notifications and communication of incidents, and the establishment of a cyber hot-line.[83]

Conventional wisdom among a group of potentially antagonist countries is first to increase transparency, then gradually proceed to cooperative undertakings – and only after that, as and if necessary, to consider restraint and security measures. Greater transparency is intended to reduce mutual suspicions and make international relations more predictable. With cooperative measures, the aim is to improve the capacity to solve problems, e.g. cyber incidents, and to build trust and confidence in the good will of the other party.

The proposed CBMs do not directly address issue of stability. Theories, regarding confidence- *and* security-building measures in particular, do recognize the importance of stability and constraints.[84] However, in the international dialogue, the time does not seem ripe for

[80] UN GGE 2013, #26.

[81] UN GGE 2015, #16–17. On confidence and stability, see Conference of Security and Cooperation in Europe, Final Act (Helsinki 1975).

[82] See for example, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies', Decision no. 1202 (PC.DEC/1202 10 March 2016).

[83] The White House, 'U.S.–Russian Cooperation on Information and Communications Technology Security' (17 June 2013).

[84] See for example, Zdzislaw Lachowski, Confidence- and Security-Building Measures in the New Europe

SIPRI Research Report No. 18, Oxford University Press (2004).

constraints and stabilizing measures.[85] The major powers are occupied with developing their capabilities and doctrines, and do not want their freedom of manoeuvre restricted even by voluntary mechanisms. In a conflictual situation, achieving transparency and cooperation is difficult: the parties lack trust and certainty regarding the future. Restraint, on the other hand, is needed. Some measures – for example, restraints on dangerous and destabilizing practises like naming and shaming, targeting and offensive exercises – can be taken relatively quickly. They are verifiable, and, if needed, can be reversed.

In cyberspace it is possible to apply targeted transparency and restraint measures, similar to the case of conventional and nuclear domains. 'Cyberspace' is actually a metaphor, and many activities are virtual – but any national cyber capability requires facilitating capability elements that can be subjected to international scrutiny. Trends, volumes and changes in the development of the cyber capabilities of national and defence forces can be observed and reported; greater transparency here can reduce insecurity over intentions and capacity.[86] For example, information on cybersecurity and cyber military strategies, doctrines and action plans should be collected in an international depository. Visits and inspections to cyber commands and cyber specific units as well as to national and international cyber exercises should be made possible, and later mandatory. Moreover, disputes, conflicts or crisis are real world ones: any ICT of the cyber dimension is but a character, not their actual nature.

Building capacity and resilience

Three consecutive GGE reports have acknowledged the vital importance of capacity-building in ensuring global ICT security, in assisting developing countries in their efforts to enhance the security of their critical national information infrastructure, and in bridging the divide in ICT security; moreover, according to the 2010 report: 'the varying degrees of ICT capacity and security among different States' is seen as increasing the vulnerability of the global network.[87] The 2013 and 2015

[85] Note that the element of restraint is missing in the CBMs adopted in the UN GGE and OSCE. Similarly, the US policy oos focused on transparency and cooperation measures. See, for instance, US International Strategy for Cyberspace, The White House (May 2011), p. 9, or https://osce.usmission.gov/on-the-adoption-of-a-second-set-of-cyber-confidence-building-measures-statement-to-the-pc/.

[86] Eneken Tikk, 'Cyber: Arms Control without Arms?' in Tommi Koivula and Katariiina Simonen (eds), Arms Control in Europe: Regimes, Trends and Threats (Helsinki: National Defence University, 2017), pp. 151–170.

[87] UN GGE 2010, #11, 17.

reports have deepened the elaboration and provided recommendations for action, including:

(a) securing ICT use and ICT infrastructures; strengthening national legal frameworks, law enforcement capabilities and strategies; combatting the use of ICTs for criminal and terrorist purposes; and assisting in the identification and dissemination of best practices;
(b) creating and strengthening incident response capabilities;
(c) supporting the development and use of e-learning, training and awareness-raising with respect to ICT security to help overcome the digital divide; and
(d) increasing cooperation and transfer of knowledge and technology for managing ICT security incidents, especially for developing countries.[88]

Many industrialized countries have now put cyber capacity-building on their agendas. The EU has a specific Instrument for Stability which addresses cyber security capacity-building in the areas noted by the Council of Europe Convention for Cybercrime: judicial and law enforcement training, and assistance in creating technical and organizational incident response capabilities.[89] Clear examples of linking cyber capacity-building to international peace, security and stability are the international cyber strategies of Australia,[90] the Netherlands[91] and Norway.[92]

However, as currently offered and demanded, cyber capacity-building has rather limited and indirect effects on stability. True, it helps to create basic IT and ICT capabilities in developing countries. Established and supported entities are able to maintain the functionality of national systems and conduct basic incident emergency responses. Economic and societal opportunities are created, and perhaps local, regional and global digital divides are being narrowed, as well. However, without long-term commitment, and holistic vision linking desired outcomes and relevant priorities about technologies transfers

[88] UN GGE 2013, #30, 32; cf. UN GGE 2015, #19-21.

[89] European Commission, 'The Instrument contributing to Stability and Peace responds rapidly to crises, builds peace and prevents conflict around the world', https://ec.europa.eu/fpi/what-we-do/instrument-contributing-stability-and-peace-preventing-conflict-around-world_en.

[90] Australian Government, International Engagement Strategy (2017).

[91] Ministerie van Buitenlandse Zaken, 'Digitaal bruggen slaan'. Internationale Cyberstrategie naar een geïntegreerd internationaal cyberbeleid (2017).

[92] Utenriksdepartementet, Internasjonal cyberstrategi for Norge (2017).

and investments in professional and academic education there can be no *sustainable* capacity.

Capacity-building comes with coded values. 'Combatting cybercrime' may sound neutral – but the Convention on Cybercrime of the Council of Europe as been rejected by some countries as patronizing, post-colonial and intrusive.[93] Moreover, the industrialized countries are advancing more rapidly than those of the Global South. The digital divide is becoming a performance gap, furthering changes in the regional and global balance of powers. [94]

To maximize the stabilizing effects of capacity building, states could set resilience as the key objective of their capacity-building efforts. Indeed, the 2013 UN GGE report identifies 'resilience' as one of the overall goals and characteristics of the desirable ICT environment central to all its recommendations.[95] Resilience, understood as the ability to bounce back, recover from disturbances, is a key characteristic of a stable cyber-political and cyber-physical environment. Obviously, resilience builds upon being able to repel an existential disaster, but it requires political, organizational and technical continuity of operations. Resilience measures are defensive by nature. They do not threaten anyone, and are incapable of shielding offensive intentions or capabilities – a concern familiar from the nuclear setting. Achieving an appropriate level of resilience requires not only accurate analysis of one's own vulnerabilities and the potential disturbances, but also systemic robustness, individual skills and the organizational capacity to handle disturbances, with practiced operational procedures and, to certain extent, backup or substitute means and measures. No country can ever be fully equipped for this: appropriations are always less than absolute, and are proportional at best.

[93] Also known as the Budapest Convention is said to be "the most relevant international agreement on cybercrime and electronic evidence". The Convention is complemented by a follow up mechanism and by capacity building programmes, supporting the Convention to remain relevant despite societal and technological changes. (Alexander Seger, "The Budapest Convention on Cybercrime: a framework for capacity building", Global Forum of Cyber Expertise (7 December 2016), available at https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime.)

[94] Niels Nagelhus Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South' Third World Quarterly. 36(5) (2018): 82-837.

[95] UN GGE 2013, #11-15. The 2016/2017 Group is reported to have discussed resilience in the context of risk assessment and business continuity and the protection of national and cross-border critical infrastructure.

If arms control and non-proliferation measures of stability remain out of reach in the international dialogue, attention could be turned to the effect of more general mechanisms of access to science and knowledge, cooperation, understanding of the threat situation and maximizing shared benefits. States must recognize their unique threat and opportunity formulas and the resultant requirement of resilience, even strategic autonomy, in seeking external assistance.

In conclusion: recommendations for optimizing stability

Stability is never absolute or set in stone. Each entity carries the elements of its own change, perhaps even its destruction. Furthermore, stability measures – like any political choices – involve deliberate risk-taking and imperfect measures, limited by their scope and effect.

There is no universal stability – or formula for such a thing. The values and objectives of the real-world politics of stability are contingent. Even the most directly technical recommendations for increasing systemic stability encounter the political imperatives of influence, power and resource allocation. The various measures examined above show clearly there is no single path to international peace, security and stability. Indeed, any individual measure on its own might become a destabilizing factor. The objectives and measures of stability become accepted as real and true only by means of negotiations. In such negotiations, countries' positions on stability are conditioned by their national ambitions and preferences as to the means and ways to achieve those ambitions, and stability, as necessary.

Those who genuinely seek stability must not leave its framing to chance. Guidance for behaviour aimed at producing greater stability should, at the very least, explain what the proposed norms are intended to achieve, and how; and how these outcomes relate to international and national stability. Account must also be taken of the feasibility of implementing the proposed norms without adversely impacting the balance of markets and technical solutions. Without such assessment, and relying on best-guess approaches, it is impossible to guarantee a move towards stability. In a worst-case scenario, further instability may be created.

Combining the domestic, strategic and technical imperatives of stability, a minimum task of international stability measures can be defined as follows: to create conditions in which serious political-military conflict can be averted, international political relations are continued, and the functionality of global techno-strategic systems, networks and processes is maintained. Therefore, each proposed stability measure, be it a norm, CBM, capacity building effort or proposed interpretation of law, requires a three-step test: does it contribute to the prevention of conflict, does it constitute a desirable international practice and invoke international cooperation, and is it compatible with the technical reality, or proposes a feasible way to adjust it in ways that adheres to all three objectives.

This is, however, only a minimalist reading of stability of cyberspace, as it focuses on the avoidance of major catastrophes and a devastating war 'in our time'. A maximalist reading would call for tools to accommodate and embrace change: more sustainable stability, encompassing the concerns of human life and societal empowerment. In any case, all the three legs of stability, *peace*, *equality* and *functionality* need to be firm. Despite their mutually amplifying relationship, the three dimensions are analytically distinct, as they assume different agent–structure relationships, entail different empirical challenges and imply different solutions.

Today's emphasis on voluntary non-binding norms, rules and principles is amenable to both the USA and Russia, otherwise acknowledged as fierce rivals in the international cyber dialogue. Washington has no desire for any kind of 'cyber treaty', and Moscow wants to avoid authoritative references to state responsibility, International Humanitarian Law, and self-defence in the ICT environment. Avoiding, not answering, open questions of the applicability of international law in cyberspace, the USA and Russia effectively control the global operating environment. Other governments are flooded with the views of global commissions and conferences, contrasting scholarly pronouncements, competing governance models, and technological assistance packages, all aimed at ensuring the desired kind of 'modernity'.

In this game of influence, stability is as much being shaken as it is claimed to be sought after. The emphasis on sub-optimal solutions supports the reckless cyberspace operations of the most powerful and the most eager governments. This opportunism is in fact a manifestation of cyber-brinkmanship where the assumed void of rules and responsibilities is exploited, and the tolerance of others is tested. The hope is to forge a new equilibrium without being caught – and without major catastrophes.

The vast majority of governments do not subscribe to this military-dominated reading of cyberspace, international law and confidence building.[96] Most governments have no intention of becoming engaged in

[96] Mika Kerttunen & Eneken Tikk, 'A normative analysis of national cyber security strategies' (: https://eucyberdirect.eu/wp-content/uploads/2019/04/kerttunen_tikk-normative-analysis-of-stategies-april-2019-eucyberdirect.pdf).

aggressive cyberspace operations: indeed, they have their hands full, trying to deal with sustainable development, economic prosperity and human and societal empowerment. They do not need the sub-optimal peace, security and stability measures that wish major catastrophes away. What do they need? – optimal peace, security and stability to resist and recover from human-caused technical incidents, the negative effects of cybercrime and the harmful effects of a few indifferent governments. Never among the fittest, these governments need the most advanced form of stability in order to survive: the ability to accommodate change. Today's global politics of stability cannot guarantee this.

States must take stability in cyberspace seriously. Emphasizing the continuity of operations and stability as accommodating change, we propose the following package of normative and capacity-enhancing measures. No single measure can solve the problem.

On the normative side, the military-heavy narrative and politics of cyber affairs must be replaced with an agenda for peace and development. Simultaneously, there must be greater efforts to strengthen the international and domestic rule of law, including the development of international law in behaviour in and through cyberspace. The aim of this dual move is to return to the promise of ICT as tools of peace and prosperity, a promise that had been lost amidst the events in Estonia 2007, Georgia 2008, Stuxnet, the Snowden revelations, Cambridge Analytica, and the ruthless practice of cyber espionage. This move is what UN Secretary-General António Guterres outlined with his September 2018 *Strategy on New Technologies:* a deepening understanding of how new technologies can be used 'to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN *Charter*, the *Universal Declaration of Human Rights* and the norms and standards of International Laws'.[97]

The Internet must be kept free, open, safe and united. We need to support the continuation of expert and multi-stakeholder-centric Internet governance model, with its established track record of maintaining and developing the Internet. Any deviation from this model is likely to exacerbate the digital divide – reducing the economic and societal promise of the Internet and leading to insecurity and instability. True, China and Russia have chosen a path that effectively controls and limits flow of information across and within their on-line and off-line

[97] United Nations, UN Secretary-General's Strategy on New Technologies (September 2018).

borders. Their approach is lucrative to those who believe that digitalization is dangerous and that cemented solutions offer best stability. We recognize competing cybersecurity governance models emerging, but question the sustainability and stability of closed systems. However, if we fail on one Internet, an effort must be undertaken to establish a compatibility regime that maximises the elements of freedom and openness in networked systems.

For dealing with recurrent crises and conflicts, institutionalized mechanisms must be established that regionally and globally address issues of political and technical instability. The former includes the continuation of global and/or bilateral cyber consultations; the latter not only transparency and cooperation but also the greater application of stability-enhancing restraint measures. Importantly, preventive diplomacy – not responses or countermeasures – must be acknowledged and developed as the primary toolbox for international relations in today's world. It is also time to consider the role of the existing institutions, such as the UN Security Council, in examining and addressing the sources and implications of crisis and conflict in cyberspace.

To enhance national cyber capacity, we recommend *resilience first, and resilience for all*. The world's developing countries lack the financial, human and technical means to maintain and upgrade their technologies. To avoid deterioration of local and global connectivity, thereby losing its political and economic benefits, the West needs to launch robust and sustained transfers of advanced technology aimed at bridging the digital divide and the concomitant injustice and insecurity. Technologies are needed – to safeguard and sustain networks and services, but also to establish robust and resilient platforms across society, making it possible to achieve vital developmental goals. Technology alone is insufficient: investment in the development of individual and organizational skills, competences and performance is needed – without the newly trained workforce migrating to the West. This bold move will also help to undermine the Russian and Chinese promotion of stricter governmental controls.

No single measure or feature is in itself 'stabilizing' or 'destabilizing'. However, greater transparency about the root causes and modalities of ICT vulnerabilities as well as cyber operations can be expected to have broader stabilizing effects, triggering more focused efforts, at the national and international levels, to detect and eliminate acute sources of threat and insecurity.

To support this technological surge, domestic, regional and global dialogue and enhanced cooperation on matters of ICT development and employment must be maintained. Basically, we need to ensure the continuity of technical and political operations to handle threats and incorporate technical and societal development. This work calls for international capacity-building that applies known standards and criteria, while being sensitive to contingent needs. Finally, capacity and stability rest on human cognition. Academic and professional programmes for the maintenance and development of systems and services must inculcate norms of normalcy and decency, and emphasize non-escalatory solutions to destabilizing incidents.

As long as there is no shared understanding of what the problem is or the issues that the proposed measures are to prevent, solve or mitigate, any answers inevitably remain conditional and limited. Conceptually, and seen from a systemic perspective, stability has intrinsic, absolute value in its own right. In practice, and seen from actor perspectives, stability becomes instrumental, contingent – and always imperfect. Any stability argument or measure will always be based on the fundamental values and belief system of the speaker in question. Demonstrating (and asking) how respective national proposals achieve or meet the goals of conflict prevention, friendly relations and technical feasibility at one and the same time would take the international dialogue to a much more constructive level.

Norwegian Institute
of International
Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 OSLO
www.nupi.no | post@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

D. Soc.Sc. Mika Kerttunen is Director of Studies, Cyber Policy Institute (Tartu, Estonia), and Senior Research Scientist at the Department of Software Science, Tallinn University of Technology.

D.Jur. Eneken Tikk is Senior Research Scientist at the Department of Software Science, Tallinn University of Technology.

This report is published by NUPI's Cyber Security Centre with financing from the research project GAIA.