A BALANCE OF POWER IN CYBERSPACE

AUTHORS: DR. ALEXANDER KLIMBURG & LOUK FAESEN

1. INTRODUCTION

Cyberspace[1] is managed by stakeholders from civil society, the private sector, and, to a lesser degree, by governments. The latter, however, is increasingly asserting its role in cyberspace, leading to a redistribution of power in which States are not only competing with other stakeholders, but also amongst each other. All cyberspace users thus face a power struggle between States that stands to affect the private sector and civil society, the multi-stakeholder approach to managing Internet resources, and therefore cyberspace writ large.

This article appropriates a realist model in international relations– the balance of power theory (BOP) – and adjusts it with neoliberal concepts of power to help better understand the challenge of stability between States in and on cyberspace. It specifically enables the "cybered" international relations of governments to be analysed against the backdrop of the complex ecosystem of stakeholders. This does not presuppose that States are or should be the most important or influential actors in cyberspace. Instead, this article focuses on State interests. It identifies two conditions of the BOP theory and applies them to cyberspace in three different scenarios previously suggested by States, and offers one suggestion on the way forward.

2. THE BALANCE OF POWER

> "The greatest need of the contemporary international system is an agreed concept of order. In its absence, the awesome available power is unrestrained by any consensus as to legitimacy... without it stability will prove elusive".[2]

The balance of power theory is one of the most enduring and protean concepts in international relations.[3] It has also sometimes proven to be the battle line between both neorealist and neoliberal interpretations in international relations scholarship. This largely has been because of different interpretations of the term "anarchy" in international relations, and different assessments of the propensity of States to actually collaborate, besides a fundamentally different assessment of what constitutes "power". This has

[1] US National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."

[2] Henry Kissinger, "Central Issues of American Foreign Policy", 1969, available at: https://history.state.gov/historicaldocuments/frus1969-76v01/d4

[3] For an overview of the evolution of the balance of power theory, see Rendall L. Schweller, "The Balance of Power in World Politics", May 2016, Oxford University Press, USA. For examples of the competing theoretical and empirical claims see J. A. Vasquez and C. Elman (Eds.), "Realism and the balancing of power: A new debate." Saddle River, NJ: Prentice Hall.

sometimes amounted to wasted opportunity, since it is possible to apply more neoliberal views to BOP, both by stressing the importance of institutions as well as including a wider concept of power per se. This is even possible when taking many neorealist positions as a starting point.

For instance, a common point of departure for BOP is the basic assumption that States act rationally to maximise their security or power in anarchic systems without a higher authority to regulate disputes.[4] Robert Jervis lists four realist assumptions that constitute the foundation of this premise: (i) all states must want to survive, (ii) they are able to form alliances with each other based on short-term interests, (iii) war is a legitimate instrument of statecraft, and (iv) several of the actors have relatively equal military capabilities.[5] The system ensures that any one State's power will be checked by a countervailing (coalition of) power that is alarmed by the potential hegemonic threat it poses to the system. From here on forward, the perspectives on the BOP theory diverge: one of them views the active goal of States as pursuing strategies designed to maintain the balance, while another maintains that it is an automatic consequence of State behaviour, a side-effect.[6] As its name implies, the distribution of power, usually defined in terms of military capabilities, is central to the BOP theory.[7] In particular, rough parity among several competing actors is frequently posed as a necessary feature of such a system. Even though the invisible hand of the balance of power regulates the system, States must be moved by explicit concerns over a potential hegemon and be ready to counter it with checks and balances as they struggle to curb the rise of a potential hegemon. As we shall see later, this becomes complicated if one departs from the realist definition of power as being purely military and adopts a wider understanding of what power may entail.

Fundamentally, the balance of power is based on a compromise – it cannot satisfy every actor in the international system completely. It works best when it keeps one State from predominating and prescribing laws to the rest, and prevent the aggrieved parties from seeking to overthrow the international order. It does not purport to avoid crises or even wars. Its goal is not aimed at reaching peace, but rather moderation and stability.

> "Paradoxically, the generality of dissatisfaction is a condition of stability, because were any one power totally satisfied, all others would have to be totally dissatisfied. The foundation of a stable order is the relative security – and the relative insecurity – of its members."[8]

[4] See for example Mearsheimer: "The international system creates powerful incentives for States to look for opportunities to gain power at the expense of rivals, and to take advantage of those situations when the benefits outweigh the costs" (John Mearsheimer, "The tragedy of great power politics", 2001, New York: Norton); and Morgenthau: "the aspiration for power on the part of several nations, each trying to maintain or overthrow the status quo, leads of necessity, to a configuration that is called the balance of power and to policies that aim at preserving it", (Hans Morgenthau, "Politics among nations: The struggle for power and peace" (4th ed), New York: Alfred Knopf).
[5] Robert Jervis, "Cooperation under the Security Dilemma",1978, pp.186-189.
[6] Waltz, for instance maintains that "these balances tend to form whether some or all States consciously aim to establish and maintain balance, or whether some or all States aim for universal domination" in Waltz K.N., "Theory of International politics", 1979, Reading, MA: Addison-Wesley, p.119; and Morgenthau who considers a balance of power as a result from a State's policies in Hans Morgenthau, "Politics among nations: The struggle for power and peace" (4th ed), New York: Alfred Knopf. Statecraft based on balancing polices has been lauded by figures such as Metternich, Castlereagh, Churchill, and Kissinger.
[7] Schweller, R. L.."Unanswered threats: Political constraints on the balance of power", 2006, Princeton, NJ: Princeton University Press: "Balancing means the creation or aggregation of military power through either internal mobilization or the forging of alliances to prevent or deter the occupation and domination of the State by a foreign power or coalition. The State balances to prevent the loss of *territory*, either one's homeland or vital interests abroad (e.g., sea lanes, colonies, or other territory considered of vital strategic interest). Balancing only exists when States target their military hardware at each other in preparation for a possible war."
[8] Henry Kissinger, "A World Restored: Metternich, Castlereagh, and the Problems of Peace 1812-1822", 1957.

2.1 DEFINING CYBER POWER

Traditional understanding of the balance of power where States seek to survive as independent entities in an anarchic global system can seem particularly challenged when confronted with the concepts of *cyber power*. In a contemporary world with powerful norms against conquest, States no longer fear the same degree of physical extinction. The empirical evidence of limited military intervention for balancing purposes attests to the need to expand the traditionally military-security notion to include a wider range of means – including not only economic but also "soft power" factors.[9] Indeed, the challenge is that in cyberspace many (but not all) of the traditional realist measures of State power do not seem to hold up, and it is therefore necessary to reconceive of what power means in cyberspace.

Power, however elusive and difficult to measure, goes beyond the physical or military supremacy over another. Joseph S. Nye offers guidance by describing *cyber power* as a unique hybrid regime of physical properties (the infrastructures, resources, rules of sovereignty and jurisdiction) and virtual properties that make government control over the former difficult. Low-cost attacks from the virtual or informational realm can impose high impacts and costs on the physical layer. The opposite is also true; control over the physical layer can have territorial and extraterritorial effects on the virtual layer.[10] Daniel Kuehl defines *cyber power* as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[11] In line with his distinction between hard and soft power, Nye conceptualises three faces of power: (i) the *coercive* ability to make an actor do something contrary to their preferences or strategies, (ii) *agenda setting* or framing to preclude the choices of another by exclusion of their strategies, and (iii) *shaping* another's initial preferences so that some strategies are not even considered.[12] This article focuses on the first face, gives a cursory glance at the second, and only touches upon the third. This is not a reflection of relative importance of the respective faces of power (indeed some scholarship might consider the opposite to be the case), but rather a focus on the measurability (or at least observability) of the faces of power: the third face is difficult to capture using traditional international relations methods.

The *hard power* manifestation of the first face of power in cyberspace, which comes close to the realist interpretation of power, is the ability to infringe on the availability and integrity of data. This can be accomplished either through denial of services (e.g. DDoS) or by various methods designed to influence data integrity (e.g. destructive malware insertion by various means). To accomplish these activities, some capability is often equally required in the non-kinetic field of "espionage" – i.e. the ability to violate the confidentiality of data. This precursor, formally known as Computer Network Exploitation (CNE)[13], has since been refined to include capabilities known as ISR (intelligence, surveillance and reconnaissance) and OPE (operational preparation of the environment, a.k.a. "preparing the battlefield").[14] Thus, it is logical that the capability of States to inflict kinetic-effect harm in cyberspace requires (to various extents) the ability to

[9] See Joseph S. Nye, Jr.,"The Future of Power", 2011 *Public Affairs.*
[10] Joseph S. Nye, Jr., "Cyber Power", 2010, Harvard University Belfer Center for Science and International Affairs, pp.7-8. Available at: www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.
[11] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in: Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (eds.), "Cyberpower and National Security", 2009, Washington, D.C.: National Defense UP. Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.
[12] Ibid. p.10.
[13] CNE was initially defined in JP1-02 as "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks." In JP 3-13 (2012) its removal from JP-02 was approved.
[14] Cyberspace Operational Preparation of the Environment (OPE) is defined in JP3-12 (2013) as "consist[ing] of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE requires cyberspace forces trained to a standard that prevents compromise of related IC operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies."

conduct intelligence gathering.[15] However, the exact nature of these "kinetic-equivalent" effects, formally simply known as "Computer Network Attack" and now known as "Offensive Cyber Effect Operations" (OCEO)[16], is in doubt. While some cyber capabilities are reserved for the battlefield (e.g. to take out a radar to enable an air strike) and are at least somewhat defined and even considered as "cyber fires,"[17] other capabilities are less clear. For instance, OCEO targeted at a power grid could of course mean "switching off the grid". But it could also mean "destroying the grid" to many different degrees, including to the extent that it was not easily reconstitutable. And finally, it could also mean something completely different – where for instance the power grid is simply repositioned to be used as an espionage tool[18], or even as a weapon itself. This lack of clarity on what exact capabilities in cyberspace are, means that it is very difficult to describe comprehensively what the "means" (delivery systems or weapons) are. In some cases, this might seem relatively easy – Stuxnet, Flame, Duqu Shamoon, Ouroboros, and Dark Energy, come to mind as examples of somewhat classifiable "cyber weapons", but in other cases this would be much more difficult. For the purposes of arms control or similar, the lack of transparency in presumed force deployment and even the method of operation or intended effects make the task extremely difficult, at least if an "arms control treaty" is the goal. At best, a "cyber weapon" remains a weapon system of "omni-use" technologies that is extremely difficult for another State to verify due to a lack of transparency. Otherwise, however, States are only left with the ability to presume – basically to guess – the overall capability of another State (albeit at widely variating degrees of detail) without, in most cases, being able to detail the exact order of battle, table of equipment, tactics, techniques and procedures or other basic information – unless the intelligence assessment is very complete.

Leaving the definitional hurdles aside, the equilibrium of forces or the military balance of power in cyberspace is further complicated by characteristics unique to these tools:

- The success of an attack is more a reflection of the overall quality of defence rather than the quality of offense. An attacker will therefore always use the "cheapest" tools available, and not necessarily the most advanced.[19]
- The vast majority of offensive cyber effects can only be deployed using civilian intermediaries (networks, products) that also can be part of a neutral or even friendly third nation.
- The difference between imminent preparation for attack (e.g. OPE) and simple espionage can be hard to distinguish for the defender, making inadvertent escalation much more likely due to a failure to correctly interpret intent.
- Offensive capabilities are much cheaper and much easier to develop and deploy than the total sum of necessary defensive measures.[20]
- Unlike conventional weapons, "cyber weapons" can be re-used but are also perishable – an entire arsenal can be rendered useless without ever being used once the vulnerability is patched.[21]
- These tools are specific – the outcomes are dependent on the victim's network – and can be immediate or time-delayed. They upend conventional ways of response.

[15] Network attacks are usually preceded by network exploitation. As former NSA and CIA director Michael Hayden states in his book, "Playing to the Edge" (2017): "Reconnaissance should come first in the cyber-domain. … How else would you know what to hit, how, when — without collateral damage?"

[16] Offensive Cyber Effects Operations (OCEO) is defined in PPD-20 as "Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks."

[17] See FM3-38 (2014) for examples. Electronic Attacks, for example, is "considered a form of fires" (see 4-3).

[18] Exploiting, for instance, the ability to conduct differential power analysis on individual computers.

[19] Alexander Klimburg "The Darkening Web: the War for Cyberspace", 2017, Penguin Press.

[20] Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.", 2016,*International Security* 41, no. 3. Slayton argues that this perception leads to unnecessary escalation and militarization of cyberspace. According to Klimburg (2017), using DDoS costs as a point of departure, defense can be conceived as being up to 1,000 times more costly than offense.

[21] In "Zero Days, Thousands of Nights" by Lillian Ablon and Timothy Bogart of RAND, the average lifespan of zero-days is set at 6.9 years, and 'for a given stockpile of zero days, about 5.7 percent will be publicly disclosed after one year. The report is available at: www.rand.org/pubs/research_reports/RR1751.html.

- They can also be reverse engineered, weaponised and re-used by the victim or another party that gets their hands on the technology.[22]
- They do not only undermine the target's security, but also compromise the security of other actors using systems with the same vulnerabilities.[23]

These is just a small range of examples describing how the fundamental differences between cyber and conventional weapons greatly complicate the process of parsing State offensive cyber capabilities.

But even in the physical world, Kissinger states that "an exact balance is impossible, and not only because of the difficulty of predicting the aggressor. It is chimerical, above all, because while powers may appear to outsiders as factors in a security arrangement, they appear domestically as expressions of a historical existence. No power will submit to a settlement, however well-balanced and however secure, which seems totally to deny its vision of itself."[24] Power is thus conceived and assessed not merely as a mathematical exercise (the number of weapons or military capabilities), but takes into account the perception of a nation's leaders, the quality of its strategies, military doctrines, and its will to use power effectively. Therefore, the common perception of a State's cyber capabilities, even if founded on incomplete knowledge, can function as a basis for calculating the respective balance of power.

2.2 LEGITIMACY

According to Kissinger's theory, a balance of power is not in itself an adequate basis for order. It is regarded as a minimal condition, but if it becomes an end in and of itself, it becomes self-destructive: "a system based purely upon power will turn every decision into a contest of strength, whereas the essence of stability is the recognition of limits by major actors."[25]

If nations desire peace, they cannot seek it directly. Instead, they must focus on creating stable relations among nations, which, according to Kissinger, is based on two major conditions: the existence of a balance of power and the acceptance of an international system of mediation and legitimacy by the major powers – an acceptance he terms "the legitimizing principle" or "the principle of legitimacy". These two terms should be conceptualised as conditions that form the basic hypotheses about the ideal conditions for the effective functioning of the system.[26]

> "A balance of power makes the overthrow of international order physically difficult, deterring a challenge before it occurs. A broadly based principle of legitimacy produces reluctance to assault the international order. A stable peace testifies to a combination of physical and moral restraints." [27]

[22] The EternalBlue exploit is a good example of a weapon or exploit developed by the NSA that was leaked by the Shadow Brokers, and was used in several malware epidemics afterwards, including NotPetya and WannaCry. See for example Thomas Fox-Brewster, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak", Forbes, May 12, 2017, www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#2ff505c2e599; and Nicole Perlroth, Mark Scott, Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally", The New York Times, June 27, 2017, www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?_r=0.

[23] Several examples include NotPetya, Turla and Black Energy. These are all malware attacks generally thought to be sponsored by the Russian Federation. Nevertheless, it went rogue and the malware hit Russian organisations and companies as well. More information available at: www.cfr.org/interactive/cyber-operations

[24] Henry Kissinger, "A World Restored: Metternich, Castlereagh, and the Problems of Peace 1812-1822", 1957.

[25] Ibid. p.145.

[26] Randall L. Schweller, "The Balance of Power in World Politics", 2016.

[27] Henry Kissinger, "War Roared Into Vacuum Formed by a Sidestepping of Statesmanship", 1989, available at: http://articles.latimes.com/1989-08-27/opinion/op-1559_1_eastern-europe.

This brings us to the second condition of stability – which commonly results not from a quest for peace, but from a generally accepted legitimacy. It means no more than an international agreement about the nature of workable arrangements and about the permissible aims and methods of foreign policy. It implies the acceptance of the framework of the international order by all major powers, at least to the extent that no State is so dissatisfied that it expresses its discontent in terms of a revolutionary foreign policy. The legitimizing principle reflects the prevailing values of the historical epoch, especially how the international order should be organised in a specific context, and captures a general acknowledgement or consensus among the major actors in a system on what is considered to be the principal form of organisation and order.[28] This principle identifies the *what* – the central actors – and the *how* – the types of interactions – in the international system. The peace of Westphalia, for example, marked a change in the legitimizing principle from feudalism to the system of sovereign Nation-States. The legitimizing principle is often summarized as a "recognition of limits" by the State. It is important to understand that these limitations are not necessarily only legal or institutional, but also include the understanding of what the actual and normative reality means.

In the context of cyberspace, the system for governing global cyber activities is primarily construed within its technical reality. The various interlocking but separate governance processes that together define cyberspace have been described by Joseph S. Nye as forming a "regime complex":[29]

[28] The *legitimizing principle* is not a traditional element of the Balance of Power theory. Although the concept appears in other contexts and modes of thought, Henry Kissinger introduced it as an addition to Balance of Power in order to establish stability – see: Henry Kissinger, *A World Restored: Metternich, Castlereagh, and the Problems of Peace*. Similar definitions of the notion are included below:
"*The legitimizing principle represents the prevailing values of the historical epoch. It is in the name of the legitimizing principle that nations accept the international order."* In Gregory D. Cleva, Henry Kissinger and the American Approach to Foreign Policy, p. 66. *"By "order" is meant the legitimizing principle by which authority receives its sanction in the eyes of the association. […] It goes to the problem of discovering the operative ideals, the expectations, the rules of concerted action to which the group members believe it necessary to conform in order to give their leaders the necessary authority to realize their own desires and objectives."*
In Avery Leiserson (1949), 'Problems of Representation in the Government of Private Groups.' *The Journal of Politics* 11, no 3: 569. *"The urge for formally declared and generally acknowledged legitimacy approaches the status of a constant feature of political life. This urge requires that power be converted into authority […]. Politics is not merely a struggle for power but also a contest over legitimacy, a competition in which the conferment or denial, the confirmation or revocation, of legitimacy is an important stake. […] [t]here is, of course, a correlation between the nature of the legitimizing principle and the identity of its applicator. For instance, the principle of divine right tends to call for an ecclesiastical spokesman, and the consent theory implies reliance on a democratic electoral process."* In Inis L. Claude Jr. (1966), 'Collective Legitimization as a Political Function of the United Nations.' *International Organization* 20, no 3: 367. *"Legitimizing principles are called into question during major systemic crises, such as world wars or widespread political upheavals […]. This dynamic occurs because it is impossible to completely satisfy the statist and nationalist principles simultaneously. Therefore, the new system tends to generate its own crisis, leading to a reevaluation of the normative principle."*In SJ Barkin and B Cronin (1994), 'The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations,' *International Organization* 48, no 1: 108.
[29] Joseph S. Nye, Jr. "The Regime Complex for Managing Global Cyber Activities", Global Commission on the Internet Governance, May 2014. Available at: www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

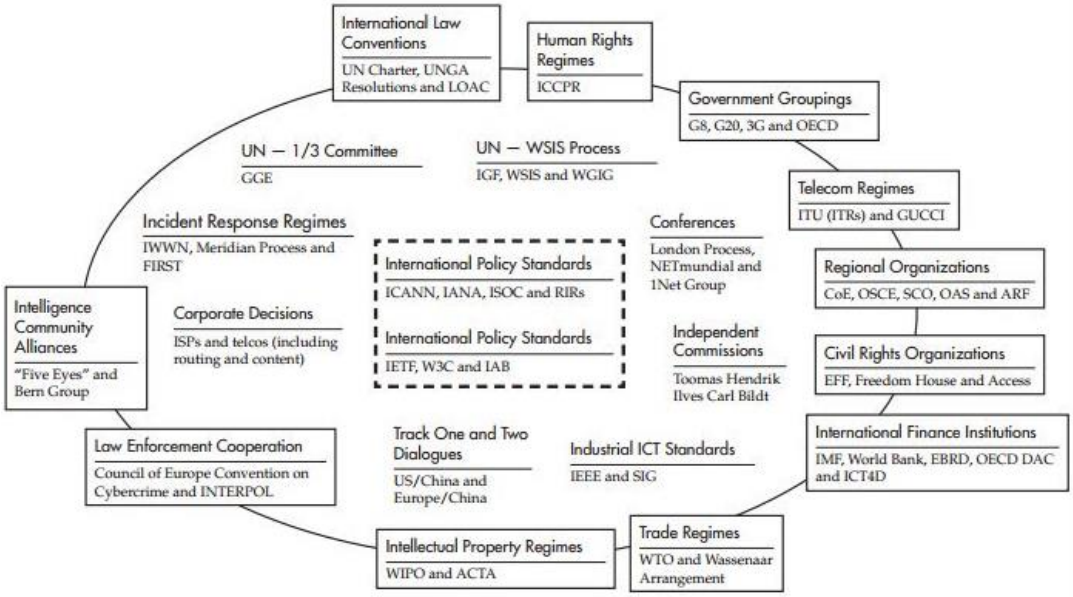

FIGURE 1. "THE REGIME COMPLEX FOR MANAGING GLOBAL CYBER ACTIVITIES". SOURCE: JOSEPH S. NYE, 2014.[30]

This regime complex is only partially influenced by State actors, and by bilateral, regional, or multilateral processes. The private sector and civil society both generate products, common practices, and norms of behaviour largely separate from government involvement, although these developments can have significant impacts on State-led processes and discussions on international peace and security. Despite States' traditional dominance over all questions related to international peace and security, governments make up only one out of three actor groups in the overall cyber regime complex, and its role within it is no greater than that of the private sector or civil society. The State-oriented regimes do not necessarily have the ability to speak on behalf of other equally crucial regimes. This creates a situation unique in international peace and security, where governments cannot decide on all aspects of the international cybersecurity domain itself, as responsibility and ownership for this domain is shared with non-State actors.

This could arguably be described as the multi-stakeholder reality of the domain. While the term does not have a single overriding definition, it does have an implicit definition. Its core idea is that some issues are too complex and have too many independent operational stakeholders to be decided on by one inevitably self-interested group and therefore require the participation of all stakeholders: civil society (including academia and technical community), the private sector, and governments. For the Internet, this is seemingly grounded in reality. It is the members of civil society (which includes State-funded university researchers, as well as corporate engineers working on their own time) who write the code of the Internet. It is the private sector that builds and owns most aspects of the Internet, ranging from the cables to the services, to products and software which runs on and in it. Government's role is relatively limited in that respect. Its power is manifested through its sovereign rights and jurisdiction.

Given this complex landscape, it is unlikely there can be a singularly encompassing entity successfully acting unilaterally across the entire regime complex. If, for instance, governments, as an overall actor group, were to agree to make definitive changes to the current non-State dominated Internet governance structures, then there would almost certainly be a strong reaction – not only from the private sector, but also from the engineers and hobbyists who have coded most of the backbone of the Internet. Installing an intergovernmental organisation instead of, for instance, the Internet Engineering Task Force, would not

[30] Ibid.

simply make these volunteers stop working on Internet technology. Therefore, the most basic reality of the wider cyber regime complex is that it is in its own, precarious, multi-stakeholder balance. While States can and may expand their own arrangements amongst each other, certain basic realities of how the domain is managed cannot be changed. Nothing that completely goes against the diffused power structure of cyberspace can therefore be considered viable or "legitimate" – the multi-stakeholder approach is therefore, in effect, the Westphalian System of the Internet.

3 BALANCING POWER IN CYBERSPACE

Thus far, it has become apparent that an equilibrium of State forces in cyberspace remains elusive because of the lack of a basic understanding of each other's capabilities and doctrines and therefore also a minimum amount of agreed definitions. Moving beyond power, the legitimizing principle reflects the recognition of the limits of States in the prevailing reality of the historical epoch. In cyberspace, this arguably can be expressed as the multi-stakeholder approach because of the technical reality of cyberspace that prevents one party from deciding universally and unilaterally.

From a State perspective, there are different ways to achieve a balance of power. In the next section, the guiding principles will be applied to three scenarios proposed by States that roughly correspond to the first three Committees of the UN General Assembly to see how likely they can actually lead to a balance of power that upholds to the legitimizing principle. This does not mean that the UN is or should be the sole means through which to establish international peace and stability in cyberspace. Instead, it offers a starting point to identify initiatives that have been previously proposed by governments, and one suggestion on the way forward.

3.1 FIRST BASKET, FIRST COMMITTEE ISSUES

The First Committee of the United Nations General Assembly deals with issues of disarmament and international security. As previously mentioned, States make up only one of the three actor groups within the overall cyber regime complex despite their traditional dominance over all questions related to international peace and security in cyberspace, meaning they cannot decide on all aspects by itself – ownership is shared with the private sector and civil society. Yet, the involvement of non-State stakeholders in the international State-led processes remains limited at best. The last UN GGE Consensus Report (described below) seems to acknowledge the need to involve other stakeholders in its conclusions: "while States have a primary responsibility to maintain a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations."[31]

Using Nye's cyber regime complex as a point of departure, one of the authors expands Joseph Nye's regime complex to offer an impression of the stakeholders and respective processes affecting the political-military dimension of cybersecurity, a.k.a. "international cybersecurity" or "international peace and security in cyberspace" that could be considered UN First Committee issues.

[31] UNGGE 2015 Report, paragraph 31 on p.13, available at www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

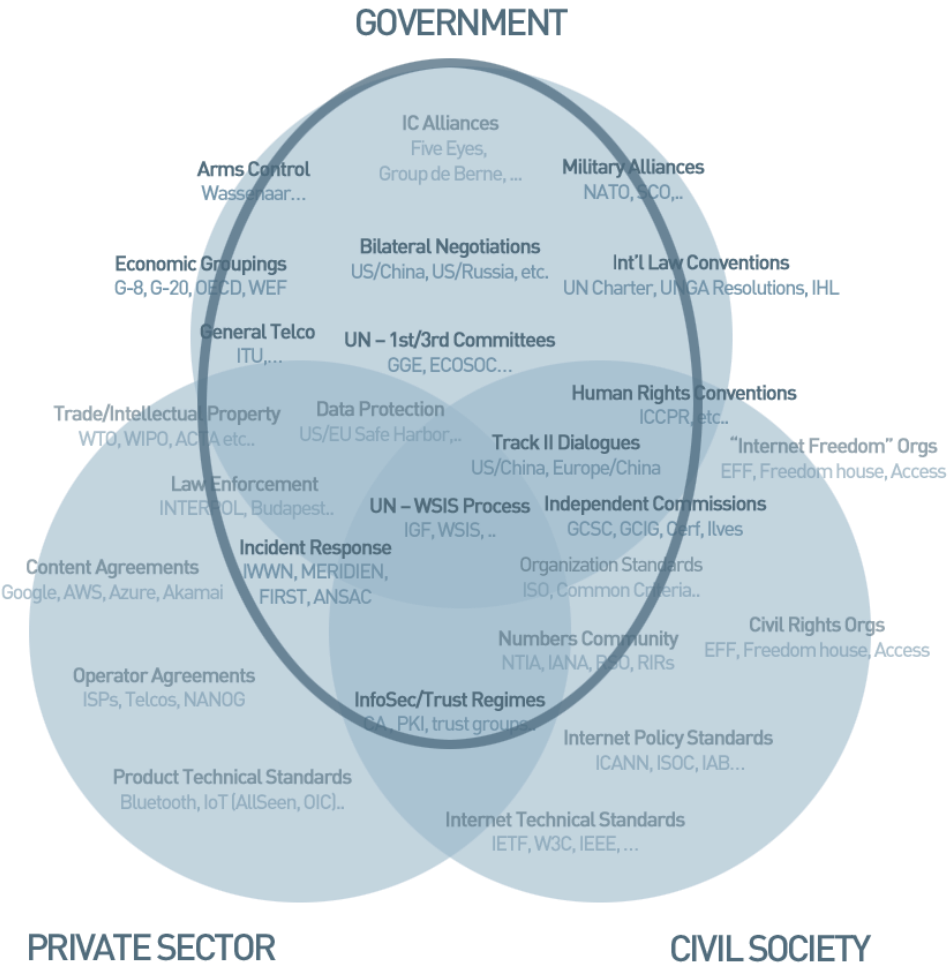

FIGURE 2. THE CYBER REGIME COMPLEX BY STAKEHOLDER GROUP: THE "INTERNATIONAL CYBERSECURITY" CLUSTER IS MARKED IN RED. SOURCE: ALEXANDER KLIMBURG, 2016.[32]

In the UN context, the First Committee is most concerned with guiding responsible State behaviour in terms of international peace and security in cyberspace. To this end, there have been three major Sate efforts in the UN:[33]

1. **The United Nations Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security (GGE)** Since its inception in 2010, the GGE has convened five times and issued three consensus reports. Each group had a mandate of only one year – which, until now, has been renewed on an annual basis. The first consensus report recommended that States consider norms, confidence building measures, and capacity building initiatives to "reduce the risk of misperception" in cyberspace.[34]

[32] Alexander Klimburg, "To the GGE and beyond…", UNIDIR Cyber Stability Conference Series, 17 July 2016, Geneva. available at: www.unidir.ch/files/conferences/pdfs/looking-ahead-the-gge-and-beyond-en-1-1173.pdf.
[33] For a comprehensive overview of cyber diplomatic initiatives see: Alex Grigsby (2017), "Overview of Cyber Diplomatic Initiatives", and Deborah Housen-Couriel (2017), "An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives", both published as Briefings from the Research Advisory Group for the Global Commission on the Stability of Cyberspace, available at: https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.
[34] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (July 30, 2010), available at: www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

In the second consensus report, major powers explicitly recognised for the first time the application of international law, in particular the Charter of the United Nations, is essential to maintaining peace and stability in cyberspace.[35] It also encouraged the development regional Confidence-Building Measures. The third consensus report outlines voluntary peacetime norms States are encouraged to follow. The 2016-17 iteration failed to reach a consensus report. The stumbling block: the application of international law to cyber operations.[36]

2. Members of the **SCO have circulated a draft international code of conduct for information security at the UN General Assembly**.[37] The code proposes that States voluntarily forego the "use of [ICTs] … to carry out activities which run counter to the task of maintaining international peace and security." It predominantly focuses on interstate cooperation against the use of ICTs to incite the "three evil –isms": terrorism, separatism or extremism, as well as reinforce the notion of non-interference in the internal affairs of States through ICTs. The code has been floated at the UN since 2011, but has attracted criticism for its perceived incompatibility with human rights law.[38]
3. Finally, the **UN General Assembly adopted a resolution in 2003**, calling on states to build a culture of cybersecurity by encouraging domestic stakeholders to be aware of cybersecurity risks and to take steps to mitigate them.[39]

Other multilateral initiatives to enhance international security and stability have been agreed outside of the auspices of the UN, most notably, the work of the Organization for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF), and other regional organisations on Confidence-Building Measures (CBMs). In addition, previous efforts have been made towards potential control of "intrusion software" by the Wassenaar Arrangement that aimed at "creating a consensus approach to regulate

[35] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (June 24, 2013), www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[36] The United States argues it failed over states' unwillingness to explain how specific bodies of international law, such as the law of armed conflict (LOAC) or state responsibility, apply to cyberspace. Cuba, echoing the views of Russia and China, argues that acknowledging LOAC would legitimize cyberspace as a domain for military conflict, giving state-sponsored cyber operations a green light. **Sources**: Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," available at: www.state.gov/s/cyberissues/releasesandremarks/272175.htm. "71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security," Cuba's Representative Office Abroad, available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information. **For a non-State expert commentary** of the failure of the 2016-2017 GGE, see for example: James A. Lewis, "The Devil Was in the Details: The Failure of UN efforts in Cyberspace", August 6, 2017, available at: www.thecipherbrief.com/devil-was-details-failure-un-efforts-cyberspace-1092.

[37] The UN General Assembly, 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) January 13, 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[38] The UN General Assembly, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General, A/66/359 (September 14, 2011), available at: www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E ; Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Net Politics (blog), the Council on Foreign Relations, January 28, 2015, available at: www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era; Sarah McKune, "An Analysis of the International Code for Conduct for Information Security," the Citizen Lab, September 28, 2015, available at: https://citizenlab.ca/2015/09/international-code-of-conduct/.

[39] The UN General Assembly, Resolution 57/239, Creation of a global culture of cybersecurity, A/RES/47/239 (January 31, 2013), available at: www.oecd.org/sti/ieconomy/UN-security-resolution.pdf.

conventional arms and dual-use goods and services."[40] It has 41 signatories that regulate the export of both conventional weapons and dual-use goods, which includes certain categories of information systems.[41] In 2013, the Member States agreed to include certain categories of intrusion software to this list.[42] Although this may bolster States against network intrusions, it also significantly impedes the ability of information security researchers to exchange findings without risking criminal proceedings.

Despite these efforts, 2017 marked the shortcomings of meaningful interstate efforts to advance norms and legal interpretations to bring international security and stability. This is just one way to do so. Some experts foresee a more fruitful future for operational cooperation – e.g. in CBMs[43], while others are exploring countering efforts to the proliferation of offensive cyber capabilities.[44]

The most promising but also most difficult application of a balance of power framework would be through the traditional area of arms control. As noted before, the notion of what constitutes a "cyberweapon" is as open and contentious as the concept behind "cyber power" per se, and there is no definition of a cyberweapon or even cyber capabilities that would lend itself to negotiations. Russia and China still view cyber threats in fundamentally different ways as the United States (e.g. information weapons versus cyber tools), making it difficult to establish and enforce such a framework. There are some workarounds that have been suggested, such as the focus on simply regulating certain "effects" rather than trying to define the weapons. However, they also stumble over some basic differences in understanding of international law.

Currently, the open questions in international law, particularly the status of data as an object[45], are almost as difficult as technical understanding of what could comprise a "weapon" in cyberspace, mainly due to the dual-use or omni-use nature of many of the potential subcomponents in a "cyberweapon", and the need for the technical community, researchers, or the private sector to be able to provide security tools for testing. However, if these hurdles can be overcome, the ability to at least agree on a counter-proliferation agreement (similar to the Missile Technology Control Regime or the Treaty on the Non-Proliferation of Nuclear Weapons) is theoretically possible. Such an agreement would clarify both concepts and capabilities of signatory States, as well as limit the transfer of those capabilities to other actors (including non-State actors). If such a treaty neither violated the need of the technical community to have simple and easy access to security testing tools, nor set a dangerous precedent by trying to "outlaw" individual pieces of code globally, then it could arguably provide for a much needed dose of predictability among States.

3.2 SECOND BASKET, SECOND COMMITTEE ISSUES

The Second Committee of the United Nations General Assembly focuses primarily on economic and financial issues, and has a strong connection to the United Nations Development Programme and the United Nations Economic and Social Council (ECOSOC). The Council is covered by the schedule officers from both the Second and Third Committees. The primary issue on the Committee's agenda is the "digital economy" – an issue predominantly discussed outside of the auspices of the United Nations, by institutions

[40] The Wassenaar Arrangement was criticized as lacking in technical expertise—partially because governments had no prior history of engaging with issues related to cyber security. For similar point see: Goodwin and Fletcher, "Export Controls and Cybersecurity Tools".
[41] More information available at: www.wassenaar.org/about-us/
[42] More information available at: www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf
[43] Alex Grigsby, "The End of Cyber Norms", *Survival*, 59(6), 2017.
[44] Robert Morgus, Max Smeets, Trey Herr, "Countering the Proliferation of Offensive Cyber Capabilities", 2017, published by the Global Commission on the Stability of Cyberspace, and available at: https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.
[45] The Second edition of the Tallinn Manual states that, in the opinion of its experts, data is not an object in legal terms (*Tallinn Manual* at p.127). This view is, however, disputed by other scholars. See for example: Michael J. Adams, "A Warning About Tallinn 2.0 … Whatever It Says", Lawfare, January 04, 2017, available at: www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says.

such as the EU, OECD, G20, G7, WEF, to name but a few. The digital economy includes specific issues such as digital trade, e-commerce, infrastructure development, and industry 4.0.

In this context, however, a closer look will be taken at law enforcement cooperation as a potential approach to establish a balance of power. Admittedly, law enforcement cooperation can also be categorised under the First or Third Committee issues. The Budapest Convention on Cybercrime established by the Council of Europe and open to third party members is one of the most authoritative in this context, but has been criticised because it seemingly enforces a Western narrative.[46] In response, Russia has reportedly proposed a draft convention on countering cybercrime and promoting law enforcement cooperation under the auspices of the United Nations, as it apparently believes previous conventions threaten the sovereignty of independent States.[47]

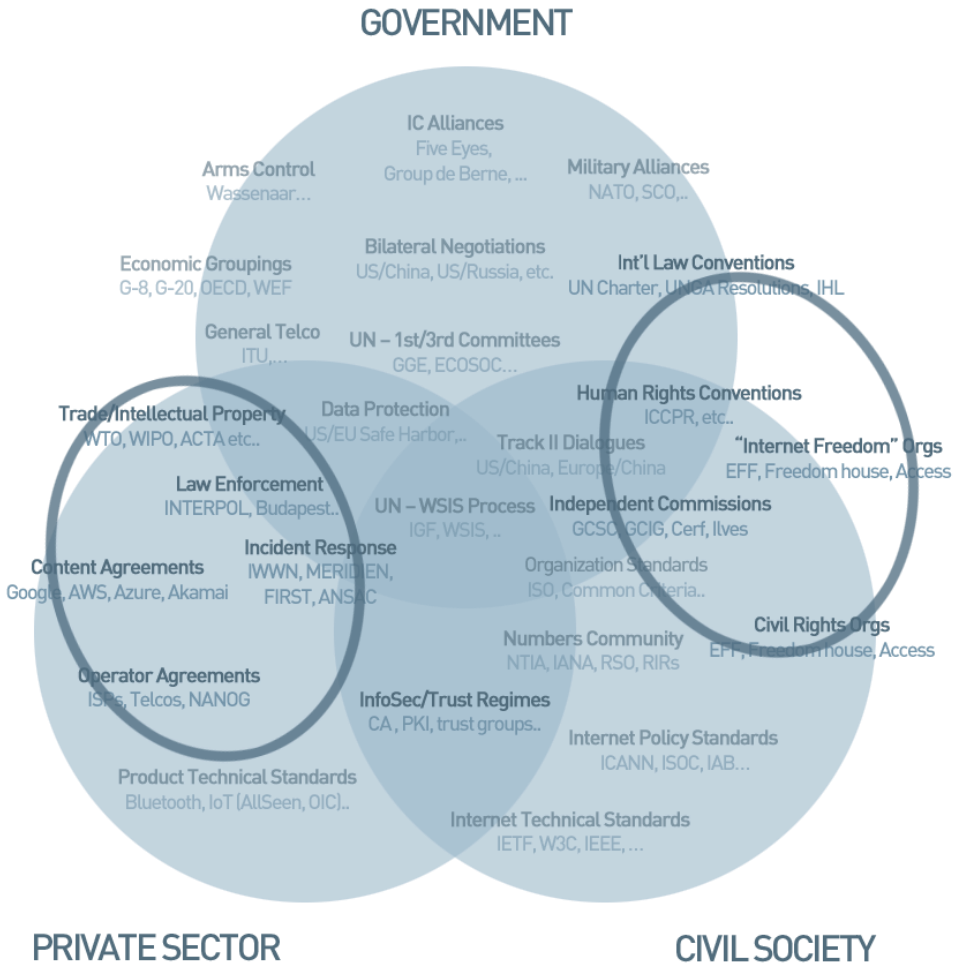

FIGURE 3. THE CYBER REGIME COMPLEX BY STAKEHOLDER GROUP: "LAW ENFORCEMENT" & "CIVIL RIGHTS" CLUSTERS MARKED IN RED. SOURCE: ALEXANDER KLIMBURG, 2016.[48]

[46] "Convention on Cybercrime", Council of Europe (2001), European Treaty Series - No 185, available at: www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[47] "Russia Presents Draft UN Convention on Fighting Cyber Crimes in Vienna", Sputnik, May 25, 2017, https://sputniknews.com/science/201705251053959333-russia-un-convention-cybercrimes/ .

[48] Op. cit. Klimburg, 2016.

The area of law enforcement cooperation offers some possibilities for pursuing a balance of power approach between States. First, in this context, the power of States is at least partially framed by the second and the third face of power considerations – co-option and conviction of soft power, besides the overall perceived coercive "hard power" strength of its suspected military and intelligence cyber capabilities. Second, a State can relatively easily ramp up its engagement in negotiations in this space, but it will be a credible actor only if it has a strong reputation in general and in the "rule of law" in particular – not necessarily the easiest of all criteria to fulfil. Third, it allows States to address the issue of malicious non-state actors that impact their national security concerns, including, for instance, countering the terrorist use of ICTs. Finally, a law enforcement approach that concentrates on mutual legal assistance treaties (MLATs), rather than specifying specific crimes, does not contradict the legitimizing principle.

The limitations of the benefits of the law enforcement treaty approach to achieve a balance of power are based upon a simple understanding of what power in cyberspace is. Such a treaty would theoretically have little bearing on a State's ability to conduct offensive cyber operations and therefore would not impact its "hard power" capabilities, unless the government in question clandestinely leverages cybercrime actors to buttress its own governmental capabilities. In the latter case, such a treaty would represent a clear loss for the cybercrime-supporting side, and a number of governments probably do fall into this category, limiting decisively their actual power gains as a well.

A law enforcement approach is theoretically possible and more likely to succeed than the arms control approach described above and the Internet governance approach that will follow below, but it falls short in what it delivers for the balancing of States. Although it does not necessarily address the hard powers of States, it deals with the contentious issue of non-State actors that governments have struggled to manage, and, more importantly, builds confidence among States. A final disclaimer would be that the proposed solutions to "double-bad" issues (illegal in both jurisdictions) can be a slippery slope for increasingly intrusive surveillance measures that the Western like-minded States would not condone.

3.3 THIRD AND FOURTH BASKET, THIRD COMMITTEE ISSUES

The Third Committee of the United Nations General Assembly focuses the social, humanitarian and cultural issues. Most notably, human rights are discussed within this Committee, and also in other UN institutions, such as the Human Rights Council and UNESCO, as well as outside the UN context: the Council of Europe, EU, OSCE, Freedom Online Coalition (FOC), IGF, WSIS, APC, Human Rights Watch, and many more. The application of international law (including human rights law) has already been established by the United Nations, and a human rights-based approach has been reiterated in many other contexts such as the NetMundial Declaration in 2014. It is, however, unlikely to create a balance of power among States by and of itself as many of the *multi-lateralist* countries that promote a State-governed Internet through notions such as "cyber sovereignty" remain critical of human rights. Moreover, human rights law governs mainly the relations between governments and their citizens. Instead, it needs to be incorporated into other approaches.

Finally, there have been several attempts by States to assert power in cyberspace by pushing for a State-led Internet governance approach through the International Telecommunications Union (ITU) of the United Nations. Internet governance is largely treated as a Second Committee issue (primarily through ECOSOC and the Internet Governance Forum) but there are options to connect it to the Third Committee as well. The IGF has no formal decision-making power or government policy-making impact, but instead helps to coordinate and facilitate among the different Internet governance constituencies. If the 3rd Committee link to Internet governance can be strengthened, this might also reinforce the notion of a rights-based Internet.

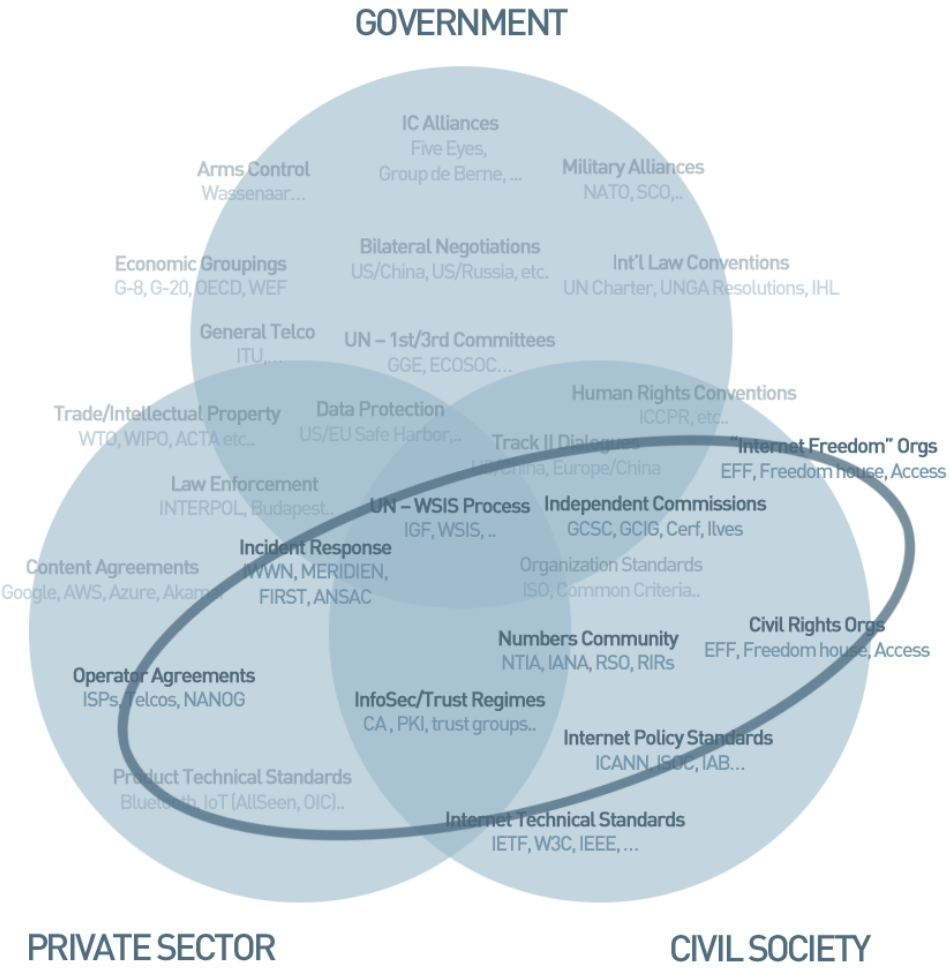

FIGURE 4. THE CYBER REGIME COMPLEX BY STAKEHOLDER GROUP: "INTERNET GOVERNANCE" CLUSTER MARKED IN RED. SOURCE: ALEXANDER KLIMBURG, 2016.[49]

The Internet governance regime complex best represents the complexity of dealing with the larger issues of managing resources and behaviours in cyberspace. It encompasses a wide range of different institutions, from established international organisations like the International Telecommunications Union (ITU)[50] to the critical Internet Engineering Task Force (IETF)[51] that is characterised by its informal structure, and the non-profit public-benefit corporation known as the Internet Corporation for Assigned Names and Numbers (ICANN)[52]. Most importantly, the Internet governance ecosystem is resolutely representative of the multi-stakeholder approach, with civil society, the private sector and government stakeholders each working more or less equally according to their strengths. As such, it is a "proof" of the legitimizing principle of cyberspace: nothing that is determined about resources and behaviours in cyberspace can be legitimate if it fully violates the basic reality of how the Internet is actually managed.

[49] Op. cit. Klimburg, 2016.
[50] The ITU is a United Nations agency established in 1865, whose mission includes developing technical standards, allocating the radio spectrum, and providing technical assistance and capacity building to developing countries.
[51] The IETF is one of the most important organizations working on Internet protocols and effectively decides much what constitutes the Internet's nervous system; most protocols, such as DNS and BGP. Its mission is to "make the Internet work better" from an engineering point of view. They try to avoid policy and business questions as much as possible, which are mostly managed by the Internet Society.
[52] ICANN is a non-profit public-benefit corporation with the purpose to coordinate at the overall level, the global Internet system of unique identifiers and manage the Internet names and addresses (IANA function) www.icann.org/resources/pages/what-2012-02-25-en,

As such, a major question of the State's influence on Internet governance was solved by a momentous decision by the Obama administration. 1 October 2016 marked a historic moment, when the US government officially cut the final strings to its influence over ICANN by handing over the IANA function – the management of the root zone file of the Internet – to ICANN in its entirety.[53] The process of slowly moving the Internet away from government influence was arguably part of the basic US approach to the Internet since as far back as the 1980s. A number of steps under various administrations conformed to this principle – slowly moving the Internet "back into the Internet community" that gave birth to it, even if that community was heavily financed by the US government in its early years. The commitment of the US government to fully disinvest itself from the last vestiges of direct control over the Internet was given new urgency after the June 2013 Snowden revelations and the significant impact this had on US "soft power", particularly in and through cyberspace. Although it marks an awkward bent in realist thinking that a State would voluntary give up power, the Obama administration made the assessment that sticking to previous political commitments and "releasing" the last shreds of government control over the Internet confirmed to three objectives, namely it reinforced the US soft power when it gave up its first "potentially coercive" face of power, to (i) gain a stronger position in the second face, i.e. in agenda setting or framing, (ii) it confirmed a self-image of the United States as a leader of a "Free Internet", and (iii) it finally reinforced the basic legitimizing principle of the Internet altogether: it is run by the multi-stakeholder approach, and no one government can exercise a hegemonic position on it. Instead, all States enjoy the same relative power. Therefore, the US IANA disinvestment played a significant role in bringing a "balance of power" to the Internet governance domain itself.

The internal balance of power within Internet governance means that it is, in effect, a poor choice for States to advance their power through this approach as it would disrupt the current system and the legitimizing principle. If a State tried to do so at the expense of the multi-stakeholder model, it would conflict with the basic reality of the domain, in which the key technical standard setting bodies, such as the IETF, are resolutely outside of governmental control and due to their voluntary nature cannot be co-opted by it. If a State tried to expand its power while at the same time maintaining the multi-stakeholder model, it would be limited to very small, incremental increases, thus limiting its attractiveness. Restructuring the Internet governance ecosystem to that of an intergovernmental structure is therefore a poor choice for States to seek a different balance of power among States as they already enjoy the same relative power under the current ICANN structure that respects the legitimizing principle of the multi-stakeholder model.

4. CONCLUSION: TOWARDS A BASKET-BASED APPROACH FOR CYBERSPACE

This article set out to assess the application of the balance of power theory to cyberspace to establish international stability and order. It did so by pursuing a more neoliberal interpretation of power. Two conditions of the balance of power theory were applied to three approaches or scenarios that roughly correspond to the first three Committees of the United Nations General Assembly, to see how they could contribute to such a stable environment, leading to the following preliminary observations.

Overall, merit can be found in the realist approach to stability and international order in cyberspace by describing it in terms of compromise and of relative security and relative insecurity. By adopting a neoliberal interpretation of the notion of cyber power, the balance of power theory can be applied to certain aspects of cyberspace. Establishing stability in this environment hinges upon the acceptance of the framework of the international order by all major powers, at least to the extent that no State is so dissatisfied that it expresses it in a revolutionary foreign policy. At least for now, the Internet governance domain enjoys a balance of power among States in accordance with the legitimizing principle. This principle, described as a "recognition of limits" by the State, is construed by the technical reality of the

[53] On 1 October 2016, the contract between ICANN and the United States Department of Commerce National Telecommunications and Information Administration (NTIA) to perform the IANA functions officially expired, handing over the stewardship of IANA functions to the global Internet community. You can read the announcement here: www.icann.org/news/announcement-2016-10-01-en.

domain inhibiting one party from deciding universally and unilaterally, arguably defined as the multi-stakeholder reality in the context of cyberspace.

However, the condition of an equilibrium of forces that lies at the core of the balance of power theory is currently impossible to establish as it requires States to have a basic understanding of each other's capabilities and therefore a minimum amount of agreed definitions as to what constitutes a "cyberweapon". In this context, compared to the other options, an arms control treaty has most to offer for the balance of power for States in cyberspace. If nearly all difficulties could be overcome, it would clarify those concepts of capabilities that are in much need of more transparency. This transparency can be delivered in the short term through Confidence Building Measures (CBMs), agreements of self-restraint or norms, but those fall short in terms of visibility, verification, and rigor in the long run compared to the former approach.

Each of the other baskets has its own specific merit, but falls short in establishing a balance of power for States in adherence to the legitimizing principle. Instead, a holistic basket-based approach could serve as an alternative. In a thought piece for the Global Commission on the Stability of Cyberspace, Wolfgang Kleinwächter describes the need, dilemmas, and possibilities of such an approach.[54] Using the context of the "Helsinki Process" of the 1970s as a source of inspiration, Kleinwächter identifies four baskets: (1) cybersecurity, (2) digital economy, (3) human rights, and (4) technology. These correspond to the previously discussed baskets with the addition of "technology". Each basket includes a different constellation of actors and constituencies involved and therefore enjoys different levels of multi-stakeholder and multilateral engagement, as appropriate.

The baskets are not "joined" or organised in a hierarchical fashion. Instead, they are brought together under a decentralised Conference on Security and Cooperation in Cyberspace (CSCC) and connected through a system of liaisons and mechanisms of reciprocal reporting to increase information exchange, cross-fertilisation, and eventually, more coherence across these topics. Like its historical precedent, each basket is negotiated individually, but remains interconnected with the others, allowing asymmetric compromises in the negotiation processes – as the British Foreign Minister argued in 1972, "if we don't lay eggs in the third basket, there will be none in the other ones either". Ideally, over time, the actions of States would balance out across all baskets, enabling not only information exchange but also a more concerted level of negotiation between States. The Conference would aim at drafting a "Final Act on Security and Cooperation in Cyberspace" (FASCC), legally non-binding commitments from governments, the private sector, civil society and the technical community.

A basket-based model inspired by the Helsinki Process could create an environment in which all major players can expand their foreign policy interests in the respective baskets, while leaving room for others to do the same, leading to a more stable situation whereby all States are equally (dis)satisfied and at the same time respect the legitimizing principle of a multi-stakeholder reality in cyberspace. No matter how likely its success, it needs to be seen as a collaborative effort where progress towards stability can be made on several fronts.

The basket-based approach is obviously just one approach that need not frame a "final answer" to the overarching problem of balancing States' interests in cyberspace. But it may form a beginning.

[54] Wolfgang Kleinwächter, "Towards a Holistic approach for Internet Related Public Policy Making: Can the Helsinki Process of the 1970s be a Source of Inspiration to Enhance Stability in Cyberspace?", 2018, published by the Global Commission on the Stability of Cyberspace, available at: https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf.

This article was originally published in the European Cybersecurity Journal Volume 3 (2018) Issue 4.

DR. ALEXANDER KLIMBURG

Dr. Alexander Klimburg is Director of the Global Commission on the Stability of Cyberspace (GCSC) Initiative and Secretariat, and Director Cyber Policy and Resilience Program at the Hague Centre for Strategic Studies (HCSS). He is a non resident senior fellow with the Atlantic Council, a former associate and research fellow of the Harvard Kennedy School's Belfer Center, and an associate fellow at the Austrian Institute of European and Security Policy. His most recent book, "The Darkening Web: the War for Cyberspace" was published by Penguin Press. Dr. Klimburg has worked on numerous topics within the wider field of international cybersecurity since 2007. He has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and Internet governance.

LOUK FAESEN

Louk Faesen is Strategic Analyst at the Cyber Policy and Resilience Program of the Hague Centre for Strategic Studies. He mainly focuses on international cybersecurity, especially legal and political norms of responsible state and non-state behavior in cyberspace. He also functions as the Project Manager of the Global Commission on the Stability of Cyberspace (GCSC) Secretariat. Louk worked previously as a Policy Officer at the Task Force International Cyber Policy of the Ministry of Foreign Affairs of the Netherlands.

ABOUT HCSS

The Hague Centre for Strategic Studies (HCSS) identifies and analyzes the developments that shape our security environment. We show the intricate and dynamic relations between political, military, economic, social, environmental, and technological drivers that shape policy space. Our strengths are a unique methodological base, deep domain knowledge and an extensive international network of partners. HCSS assists in formulating and evaluating policy options on the basis of an integrated approach to security challenges and security solutions.