ICT for peace foundation

CYBER SECURITY POLICY PROCESS

BRIEF

THE REACH OF SOFT POWER IN RESPONDING TO INTERNATIONAL CYBERSECURITY CHALLENGES

Camino Kavanagh & Daniel Stauffacher

GENEVA 2013
ICT4Peace Foundation

ICT4Peace Publishing, Geneva. 2013 Copies available from www.ict4peace.org.

THE REACH OF SOFT POWER IN RESPONDING TO INTERNATIONAL CYBERSECURITY CHALLENGES

Camino Kavanagh & Daniel Stauffacher

ICT for peace foundation

THE REACH OF SOFT POWER IN RESPONDING TO INTERNATIONAL CYBERSECURITY CHALLENGES

For several decades, international relations and strategic studies scholars have sought to develop a better understanding of the transformation and diffusion of power and its impact on strategic and international affairs. In 2006, Lawrence Freedman noted that an important transformation in strategic affairs had taken place with the end of the Cold War and the demise of the Soviet Union. He challenged the claims of the theorists of a "revolution in military affairs" (RMA) that technology-driven changes in the battlefield underway since the 1990s would transform wars between powerful states into contests marked by information dominance, highly precise weapons and information technology, thus reducing war's impact on civilian populations and infrastructure. In his writings on RMA, Freedman argued that the impact of the technological changes on the actual conduct of war "depended on the interaction of these developments with changes of quite a different type – in political affairs – which at that moment pointed away from "the decisive clash between [great] powers." Freedman insisted that the RMA failed to respond to changing political conditions and adapt its wars" which were more asymmetrical, irregular and transnational in nature and more reflective of shifting power structures within states and across regions. The terrorist attacks on the United States, Spain and the United Kingdom were evidence of this reality, as were the unexpected drawn-out struggles in Iraq and Afghanistan.

Several years later, as the effects of the September 2001 terrorist attacks on the United States dissipate and withdrawal from the Iraq and Afghanistan theatres nears completion, the discussion about a transformation in military and strategic affairs has revived. It has been driven by changes in technological factors in military doctrine and strategy; power relations between and within states; the structure of the military-industrial complex; social organization articulation of interests; and changes in the nature of the threats (real and perceived) faced by highly networked powers. At the crux of these more recent debates on transformation lies a new environment: cyberspace (or information space, depending on one's strategic narrative).[1] According

1 While definitions of cyberspace abound, there is still no internationally agreed definition. This poses serious problems and can lead to misperceptions, with many falling into the trap of 'mirroring' i.e. ascribing to the other its own analytical framework.

to US military machinery to "the wars that might actually have to be fought" i.e. the "new policy makers, the national security threats posed by the malicious use of cyberspace are today ranked above threats posed by terrorism and failed or failing states.[2] Many other states share this view and are organizing their security structures accordingly.

As threats related to the different uses of cyberspace have intensified, the policy option of inter-state war was placed squarely back on the table by US decision-makers when cyberspace was defined as a strategic domain of conflict in 2009, and a dedicated military command established shortly thereafter. Indeed, statements by senior US policy makers on the threats from cyberspace have grown increasingly hawkish since the mid-2000s, with some suggesting the almost-inevitability of war between states within a domain that, in its essence, was the US' own creation.[3] Nonetheless, war between major powers over cyber attacks or war in cyberspace remains unlikely.[4] At the same time, however, the gradual build up of cyber capabilities, underpinned in large part by the concept of information dominance for military purposes, has lead other powers to develop an offensive strategy in response, mainly played out in international fora. For example, as early as 1998 Russia tabled a resolution in the UN General Assembly's First Committee on Disarmament on *Developments in the Field of Information and Telecommunications in the Context of International Security*. The unspoken aim of this resolution was to curb the technological superiority of the United States, and slow down the development of cyber and information communication technology capabilities that could be used against other states.[5] Indeed, Russia viewed the "unprecedented level of development and application of modern, substantially new information technologies and means of telecommunication" as presenting new policy options in international affairs and matters of international security. More precisely, Russia worried that developments in the information field "would be used for purposes incompatible with the objectives of maintaining international stability and security and of observing the principles of the non-use of force, non-interference

2 In the decade following the 9/11 attacks terrorism (as well as weak or failing states where terrorism could flourish) were deemed one of the principal threats to national security and the all efforts were made to adapt different instruments of policy to respond to this challenge. See also Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence (2013). Accessible at http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

3 Dunn Cavelty, (2008); Lynn W. (2010)

4 Thomas Rid (2013), 13/9/13 7:07 AM

5 Krutskikh, (2009)

in internal affairs, and respect for human rights and freedoms."[6] The US establishment of a dedicated a strategic cyber command headed by the same person responsible for the state's main espionage apparatus – the NSA - over a decade later inadvertently pushed many states towards the Russian camp.[7] These developments stand in stark contrast to earlier discussions within WSIS and other international fora regarding the significant potential of ICTs in promoting peace and development.[8]

These challenges have emerged at a moment when the post-Cold War international "uni-polar" order is undergoing important changes with some states emerging to challenge US pre-eminence on several fronts, including governance of the Internet.[9] In some respects, the Internet governance agenda has become the center of gravity for efforts aimed at shifting information power away from the US and 'taming' its leadership on cyber security matters.[10] In addition, some authoritarian governments are seeking to regain or maintain control of information flowing through their national borders[11], including as a means to push back against Western influence or interference. In Russia for example, repeated efforts have been made in international fora either directly or via the Shanghai Cooperation Organization (SCO) to fend off potential 'information wars' that could "[harm] social, political and economic systems,

6 Krutskikh, (2009) The citation is from a letter from Russia to then Secretary-General of the United Nations, which accompanied the first Resolution on Information Security tabled in the United Nations in 1998. (A/C.1/53/3 - *Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General)*. A month later Russia introduced an edited version of the Resolution to the First Committee and after further minor revisions, the General Assembly adopted the Resolution by consensus. The United States did not back it. As noted, during the same period, China also marked an important shift in how it viewed information telecommunications.

7 Austin (2013). In February 2013, Russia itself established a dedicated function in the Ministry of Foreign Affairs aimed at responding to the political use of ICTs. Andrey Krukskikh was named Special Coordinator of this new function. The post is ambassadorial level.

8 ICT4 Peace (2005)

9 Ebert and Maurer (2013); Brzezinski (2012)

10 Ibid

11 In many countries, the expansion of the Internet following its privatization of the Internet and other ICTs came as a total surprise, particularly in those states where information had previously been controlled by the state security apparatus which in turn was linked to or part of the center of power. It was not until the late nineties that many states woke up to this reality and with the support principally of US-based multi- nationals, helped put in place mechanisms of control.

as well as spiritual, moral, and cultural spheres of other States."[12] In China, a speech by Jiang Zemin in 1998 marked the beginning of a policy anchored in information control as a means to protect the country from inter alia 'infiltration, subversive activities, and separatist activities of international and domestic hostile forces" and ensure that the "Western mode of political systems is never copied.[13] The International Code of Conduct for Information Security[14], China's signing of the Shanghai Cooperation Organization's 2009 Agreement on Information Security[15] as well as more recent developments[16] appear to confirm this policy, at least in relation to control of content. At the same time, it is evident that China recognizes the importance of the Internet to its economic development and for resolving issues of social importance, and is enthusiastically promoting its expansion.[17] Over time, such shifts may lead to a less restrictive flow of information across its Internet.

The different shifts in the balance and tools of power coupled with the complexity and confusion inherent in the uses of cyberspace have contributed to erosion of trust between states. Recent events have added to concerns of how potential missteps in cyberspace or the offensive use of cyber capabilities could exacerbate existing (and not necessarily cyber-related) tensions, potentially leading to escalation and armed conflict.[18] For example, both China and the United States have accused each other of conducting protracted cyber espionage activities; the United Kingdom has also

12 Kavanagh (2012) See also Agreement between the governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field on Cooperation in the Field of International Information Security, Art. 2, 16 June 2009; and the Code of Conduct proposed by the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan (A/66/359).

13 Goldsmith & Wu (2006) Shortly thereafter, the US company CISCO helped China lay the first bricks of its 'firewall.'

14 The code of conduct was proposed by the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan (A/66/359). As with the Convention proposed by Russia, the text notes that states should protect freedom of expression on the Internet and "have no right to limit citizens' access to information space," with the caveat that governments may, however, limit these rights "for the protection of national and public security."

15 The Agreement came into force in 2011

16 See for example the recent NY Times article *China Takes Aim at Western Ideals* http://www.nytimes.com/2013/08/20/world/asia/chin as-new-leadership-takes-hard-line-in-secret-memo.html?_r=0

17 See section V, Protecting Internet Security in China's White Paper on the Internet in China, accessible at http://www.china.org.cn/government/whitepaper/20 10-06/08/content_20207978.htm

18 ICT4 Peace (2013)

been accused of similar activities. Recent revelations of the reach of NSA espionage activities has only served to exacerbate these tensions, while also weakening the foundations upon which some of the Western arguments concerning Internet freedom and governance were built.

Moreover, the United States has developed a policy and a doctrine for offensive cyber operations.[19] In fact, offensive cyber operations have now been formalized as an additional instrument of national power.[20] It is probable that other countries are also developing these capabilities.[21] Again, while it is highly unlikely that these or similar actions will lead to hostile action or a breakdown in diplomatic relations, they still impact considerably on perceptions of trust in international relations. Such actions also sharpen perceptions of power (political, military and economic) inherent in information dominance in and beyond the theatre of war, and enhance the desirability of increasing cyber capabilities as a means to attain strategic goals. In short, they encourage competition rather than cooperation between states.

Conversely, these developments have also had the combined counter-intuitive effect of creating a form of "strategic pause" among the major powers, at least for now, and may allow for progress to be made toward a consensus on how to move forward collectively to ensure that international peace and security are not undermined by incidents in cyberspace or the use of offensive cyber capabilities against non-cyber targets.[22] In this regard, states are making significant efforts to marshal soft power - the "ability to attract or co-opt as opposed to the use of coercion or the use of force" - to reach consensus on norms for responsible state behaviour in cyberspace as well as confidence building measures (CBMs).[23] Norms in particular are important given the current geopolitical information landscape, since they can "normalize the exercise of power in cyberspace," serving as a form of deterrent for aggressive cyber behaviour.[24] Indeed, if complied with, norms can potentially "channel, constrain and constitute action through inducement and coercion; moral pressure and persuasion;

19 Presidential Directive, PDD-20 Accessible at https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf

20 Ibid. See in particular Section III, p. 9

21 ICT4 Peace (2013), Lewis (2013)

22 ICT4 Peace (2013)

23 Harvard University's Joseph Nye coined the term soft power in 1990. He used the term to describe the ability to attract or co-opt as opposed to the use of coercion or the use of force. See Nye's *Bound to Lead: The Changing Nature of American Power* (1990) and Soft Power: *The Means to Success in World Politics* (2004).

24 Deibert et al in Stevens, (2012).

and social learning and habit."[25] As noted at a recent meeting on Cybersecurity and Confidence Building Measures, CBMs can, on the other hand, serve to lay the foundation for agreeing on such norms and on measures to avoid miscalculation and escalation. They can also represent initial steps towards discussions on issues such as arms control (if warranted) and finding common ground for understanding future cyber threats in a crisis or war-like situation, such as those posed to strategic assets and critical civilian infrastructure.[26]

In June this year, the UN process on *Developments in the Field of Information and Telecommunications in the Context of I nternational Security*, initiated in 1998 within the framework of the UN General Assembly's First Committee on Disarmament, reached agreement on a range of measures aimed at building cooperation for a peaceful, secure, resilient and open Information Communications Technology (ICT) environment.[27] The report affirms the applicability of existing international law to cyberspace as well as the principal of sovereignty, and includes recommendations on norms, rules and principles of responsible behaviour by states, recommendations on confidence building measures (CBMs) and information exchange, and a series of recommendations for capacity building measures. The United States characterized the report as a "landmark consensus" on issues "of critical national and international significance," not least because state-on- state activities are becoming more prevalent in cyberspace.[28]

OSCE member states are also moving forward to reach agreement on a complimentary range of CBMs; recent discussions have led to a sense of cautious optimism that participating states will adopt a first set of cyber/ICT security-related CBMs at some point in 2013. Meanwhile, discussions on CBMs within the framework of the ASEAN Regional Framework (ARF) continue. At the bi-lateral level, the longstanding U.S.-Russian strategic dialogue recently produced an agreement on some initial CBMs. U.S.-China and UK-China consultations on international cyber security are much more recent; while yet to yield concrete results, discussions seem to be moving forward. Meanwhile, similar official consultations on cyber security issues are emerging in

25 Ibid (citing Farrel, T. The Norms of War: *Cultural Beliefs and Modern Conflict* (Boulder, CO: Lynne Rienner Publishers, 2005), pp. 10-11)

26 ICT4 Peace (2013)

27 See http://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/pdf/N1337166.pdf?OpenElement The report will be presented to the UN Secretary General during the 68th Session of the General Assembly this month.

28 US Department of State, Statement on the Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues. Available at www.state.gov/r/pa/prs/ps/2013/06/210418.htm (Accessed on 02/09/2013)

bilateral talks among other states. In addition to these developments, the government of South Korea is now preparing for the next international conference on cyberspace, which will build on the earlier efforts of the United Kingdom and Hungary to broaden the dialogue beyond state actors, and assess progress to date. These are positive developments, which provide a degree of optimism that strategic restraint may become the rule rather than the exception in matters of offensive cyber operations, even if cyber-espionage will undoubtedly continue unabated[29].

Indeed, these important steps suggest that states may be ready to move beyond earlier efforts marked by ideological differences and competing strategic interests between groups of states which hindered even minor agreements on norms and confidence building measures.[30] Only time will tell however, whether these efforts to resolve highly complex interdependent issues, and which hinge significantly on the deployment of a soft power that is increasingly losing legitimacy, will balance out the current bellicose rhetoric and displays of increasingly sophisticated cyber capabilities. The fact that these capabilities are already being used (mainly covertly) both in and outside the theatre of war to meet domestic and foreign policy goals and broader strategic objectives does not necessarily bode well; hence the urgency to make progress on CBMs, norms and other related international regimes and processes related to the malicious uses of cyberspace, and expand the discussion beyond the state to other sectors, including, but not limited to, the private sector. In this regard, deeper engagement of civil society and academia will be imperative,[31] not only on Internet governance and Internet freedom issues where their voices and actions are already well anchored, but on broader international cybersecurity, including norms and CBMs processes.[32] Such engagement would also be more in tune with the role and influence these other actors de facto play in relation to cyberspace, but which is not always recognised or welcomed.

---

29 Section developed from a June 2013 ICT4 Peace report *Confidence Building Measures and International Cyber Security*, available at http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=cab359a3-9328-19cc-a1d2-8023e646b22c&lng=en&id=167425

30 Ibid

31 For emphasis on this point, see, for example, Art. 28 of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A/68/98 (forthcoming); and Art. 36 of the Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E) available at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

32 Well known non-state initiatives include the OpenNetInitiative (ONI) which led to the series *Access Denied, Access Controlled and Access Contested* by Deibert, Paltrey, Rohozinski et al and the establishment of extensive global networks; Tikk-Ringas' proposed Ten Rules for Cybersecurity (2011) are also widely cited.

Finally, the current predominant focus on state power and state-on-state rivalry with regard to cyberspace and ICTs risks once again removing attention from the "the wars that might actually have to be fought" i.e. the more asymmetrical transnational threats faced by all states – large and small, developed or developing – around which international collaboration is potentially much more achievable in the short-term, and which could establish the basis for more effective norms in the longer-term. States must work for a balance between both approaches.

Bibliography

Austin, G. (2013), Costs of American Cyber Superiority, Web article, East West Institute

Brzezinski, Z. (2012) *Strategic Vision: America and the Crisis of Global Power.* New York: Basic Books.

Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. CSS Studie. Routledge, Taylor & Francis Group.

Ebert, H. & Maurer, T. (2013) Contested Cyberspace and Rising Powers. *Third World Quarterly.* 34 (6), 1054–1074.

Deibert, R., Paltrey G. & Rohozinski, R (2010), *Access Controlled: The Shaping of Power, Rights, and Rules in Cyberspace*

ICT4 Peace (2013), Confidence Building Measures and International Cybersecurity - Workshop Report, Geneva June 2013.

ICT4 Peace and UN ICT Task Force (2005), Information and Communication Technology for Peace: The Role of ICTs in Preventing, Responding to and Recovering from Conflict.

Kavanagh (2012), Wither the Rules of the Road for Cyberspace - Policy Brief, Cyber Dialogue 2012, Citizen Lab, University of Toronto.

Krutskikh, A. V (2009) *International Information Security: The Diplomacy of Peace - compilation of Publications and Documents.* S.A. Komov (ed.).

Lewis, J.A. (2013), Significant Cyber Incidents since 2006, CSIS

Lewis, J.A (2011), Rethinking Cybersecurity – A Comprehensive Approach, Speech given at Sasakawa Peace Foundation, September 2011

Libicki, M. C. (2011) Cyber War as a Confidence Game. *Strategic Studies Quarterly.* Spring (July 2010), 132–146.

Lynn, W.J. III (2010), Defending a New Domain: The Pentagon's Cyberstrategy, *Foreign Affairs*, 89 (5), Sept-Oct. 2010

Nye, J. Jr. (1991), *Bound to Lead: The Changing Nature of World Politics*, Basic Books.

Nye, J. Jr. (2005), *Soft Power: The Means to Success in World Politics*, Public Affairs, First Edition

Stevens, T. (2012) A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. 33 (1), 148–170.

Tikk-Ringas, E. (2011), Ten Rules for Cyber Security, Survival, Vol.53, no. 3, June-July 2011, pp. 119-132

UNIDIR (2013), *The Cyber Index: International Security Trends and Realities,* New York, Geneva.

About the authors

Camino Kavanagh

Camino Kavanagh is currently pursuing a Ph.D. at the Department of War Studies at King's College London. Her research is centred on transformation in strategic affairs, with a specific focus on how cyberspace has evolved into a domain of strategic competition between states and she engages in different initiatives and projects on this subject. Camino is also a Senior Fellow at NYU's Centre on International Cooperation and currently serving as an advisor to the Kofi Annan Foundation on the evolution of organized crime and drug trafficking in West Africa. She has worked with United Nations peace operations in Guatemala and Burundi and other international organizations in Africa, Asia, and Latin America & the Caribbean. She has a MA in Contemporary War Studies and a MA in Human Rights Law.

Daniel Stauffacher

Daniel Stauffacher, a former Ambassador of Switzerland, has a Ph.D. in media and copyright law from the University of Zürich and a Master's degree in International Economic Affairs from Columbia University, New York. After working for a Swiss publishing company, he joined the UN in 1982 and worked in New York, Laos and China. Subsequently he joined the Swiss Federal Office for Foreign Economic Affairs (Bawi) in 1990, where he was a Director for Economic and Financial Co-operation with major Asian and Central and Eastern European countries. In 1995, he was posted to the Swiss Mission to the European Union in Brussels as Counsellor for Economic and Financial Affairs. From 1999 to 2005, he was Ambassador of Switzerland to the United Nations in Geneva and New York and the Swiss Federal Government's Special Representative for the hosting and preparation of the United Nations World Summit for Social Development (Geneva, 2000) and of the UN World Summit on the Information Society (WSIS) that was held in Geneva in 2003 and in Tunis 2005. He was a member of UN SG Kofi Annan's UN ICT Task Force and is a founding Trustee of Tim Berners Lee's World Wide Web Foundation (www.webfoundation.org). Dr. Stauffacher is the Founder and Chairman of ICT4Peace Foundation (www.ICT4Peace.org), President of the Geneva Security Forum and a Board Member of the Gulf Research Foundation (GRC), Geneva. He is and serves as a Special Advisor to the UN Secretariat and the Swiss Federal Department for Foreign Affairs.

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation