Cybersecurity: Challenge and Response:
A New Generation Speaks Out

November 6, 2013
Roundtable Report

Report Outline

1. Introduction

2. A Year in Review

    2.1 The outcome of the World Conference of International Telecommunications (WCIT); and the role of the UN and other international organizations moving forward
    2.2 The report of the UN Group of Governmental Experts (GGE)
    2.3 Edward Snowden's intelligence disclosures and other forms of espionage

3. What Next for U.S. Foreign Policy? Is a New Policy Approach Required?

4. Policy Recommendations

November 2013

Dear Reader,

As this report suggests, 2013 was a significant year for developments on the cybersecurity front, with significant progress made in some key areas, and equally significant setbacks in others. These developments have strong implications for US foreign policy not least because they are taking place against a background of equally important shifts in the global strategic environment. Looking forward, the US will need to reassess its current strategy for cyberspace, placing effort and resources where and with whom they are most needed.

The exploitation of cyberspace as a theater for the deployment of novel offensive capabilities is transforming the character of warfare. Offensive cyber capabilities are increasingly being incorporated into the military equation of major and minor powers and by non-state actors. Thus, despite important developments this year, serious challenges remain, including reaching agreement on how (and no longer if) the UN Charter, international law and the laws of arm conflict apply in this new age.

The National Committee on American Foreign Policy (NCAFP) will address some of the questions raised and recommendations made in the report over the next twelve months and in doing so it will continue to involve the next generation of up-and-coming cybersecurity experts, who are vital to shaping US foreign policy in this area.

I am thankful to the experts who participated in this roundtable discussion, particularly Dr. James A. Lewis, who presided over the meeting, Ambassador Philip Verveer for his enlightening remarks as the luncheon keynote speaker, and moderators Mr. Marcus H. Sachs, Mr. Nicholas Thompson, and Dr. Jason Healey. I would also like to thank Ms. Edythe Holbrook, Vice President, National Committee on American Foreign Policy, Ms. Camino Kavanagh, Ph.D. Candidate, Kings College London, and NCAFP Cybersecurity Senior Project Advisor, and Ms. Elena Garofalo, NCAFP Program Director for their hard work in the development and execution of this roundtable session. Finally, I would like to thank Mutual of America, Mr. Kevin Backus, and Mr. John H. Bell Jr., without whom this roundtable would not have taken place.

Sincerely,

George D. Schwab

George D. Schwab
President

1. Introduction

On 6 November 2013, the NCAFP hosted a second round-table on cybersecurity entitled: Cybersecurity: Challenge and Response: A New Generation Speaks Out. The objective of the meeting was to discuss core developments in three core areas – Internet Governance; Cyber Espionage; and Cyber Warfare and their respective policy implications. From the discussion it was obvious that over the past year, three core events have converged and have the potential of reshaping approaches to cybersecurity. These events include:

- The World Conference on International Telecommunications (WCIT) meeting held in Dubai in December 2012, which confirmed the push for greater government involvement in the governance of the Internet, and is leading to the convergence of Internet governance and cybersecurity agendas. The political economy of Internet governance is also shaping governments' interest in playing a greater role, particularly a growing push to keep Internet revenues at home. Combined, the latter raise serious questions about i) what a new US narrative on Internet governance issues might look like; and ii) the role of the UN and other international organizations in the governance of the Internet moving forward.

- The report of the UN-Group of Governmental Experts (GGE) whereby consensus was reached on the applicability of the UN Charter, international law, and the principles of state sovereignty and responsible state behavior to cyberspace. As discussed at the meeting, the consensus reached on these norms and principles provides a basis for further discussion on how these apply in practice, and for deeper discussion on some of the other related agendas (e.g. Internet governance).

- The Edward Snowden revelations on the surveillance practices of the US government which have not only created or exacerbated tensions between the US, like-minded countries and others, but have also shifted attention away from existing strategic concerns regarding cyber industrial espionage that can, in the long term, have an important impact on the US economy. The revelations have also exacerbated additional concerns regarding privacy at the domestic and international levels.

These developments are political rather than technological in nature; they will have consequences for international peace and security; and are therefore increasingly shaping foreign policy agendas. These same developments have emerged against a backdrop of significant changes in the global strategic landscape that have not necessarily been considered in cybersecurity strategies:

- First, due to the backlash against some of the strategic decisions it took in the aftermath of 9/11, as well as the emergence of other powers (some with different value systems), the US is less influential today than it was a decade ago, particularly with regard to the promotion of democratic values. The NSA revelations have only served to underscore this reality.

- Second, significant transformations in the character of warfare are taking place in part due to the overwhelming imbalances in conventional military capabilities of some countries (mainly the US) vis-à-vis others; and in part due to the desire of the US to disentangle itself from the

theatres it has been militarily engaged in over the past decade; and a realization of the geo-strategic importance of Asia to which the US has turned its focus. In this regard, efforts to use cyber capabilities[1] or cyber-guided technologies such as Unmanned Aerial Vehicles (UAVs), to advance foreign policy goals and create strategic effect have become more pronounced. While some of these uses of cyberspace and cyber capabilities create distrust among nations, their effectiveness has also provoked a race between states to acquire them, thus placing additional pressure on the international system and the institutions and mechanisms responsible for managing international peace and security.

This summary report discusses the aforementioned developments regarding Internet governance, the UN Group of Government Experts (GGE) report, and the Snowden revelations against the background of these shifts in the global strategic landscape. It concludes by tabling a number of questions and recommendations regarding the future direction of US foreign policy and the place of cybersecurity strategy (i.e. a more comprehensive and pragmatic approach to international cybersecurity) within that foreign policy.

[1] Either as a form of fire, or by using content/information to effect outcomes

2. A Year in Review

2.1 The outcome of the World Conference on International Telecommunications (WCIT), which took place in Dubai in December 2012 and which highlighted significant challenges to how the Internet is and should be governed and raising questions about i) what a new US narrative or more comprehensive and pragmatic approach on Internet governance issues might look like; and ii) the role of the UN and other international organizations moving forward.

- The World Conference on International Telecommunications (WCIT) conference held in December 2012 and hosted by the International Telecommunications Union (ITU), a specialized agency of the UN, was initially organized to renegotiate a 1988 treaty called the International Telecommunication Regulations (ITRs), [2] yet it ended in a diplomatic éclat. The conference confirmed deep splits within the international community and a significant challenge to the status quo of how the Internet is governed.[3]

- As noted by the roundtable speakers, the US and a small group of Western countries raised serious concerns when it became obvious that some countries would use efforts to review the regulatory document (the ITRs) for an entirely different purpose, i.e., to create new regulations for the Internet. Usually operating by consensus and without a vote, the conference took another unexpected turn during its final days when the head of the ITU asked governments to vote on a revised treaty. In addition to this surprising twist in the conference procedures, the conference record listed some 89 states voting in favor of the proposed text with some 50 states opposing it. The latter group included the United States, most European countries as well as some African and Latin American countries. These positions have not been reconciled and it is expected that tensions among these groups of states regarding Internet governance will continue to mount in the coming period. What remains unclear in this context is how the ITU's plenipotentiary in 2014 and the election of a new ITU Secretary-General (likely from China) will affect these developments.

- Several participants suggested that the Snowden revelations, discussed below, exacerbate some of these tensions on the Internet governance agenda, providing other countries with fodder to question the US [and broadly Western] position regarding the ITRs and Internet governance in general, and reinforcing existing perceptions that the US created, controls, disproportionately benefits from and offers its intelligence agencies privileged access to the Internet. These perceptions are enhanced by the fact that online content largely reflects US legal and normative principles and cybersecurity is a large and growing problem.

- One speaker noted that one of the core issues that certain discussions at the WCIT meeting in

[2] The International Telecommunications Regulations (ITRs) are an old treaty developed in the 1980s and have been re-negotiated several times since then. They were last negotiated in 1988 and they are essentially put in place to facilitate the exchange of international telecommunications traffic across borders as a way to help interconnect the world in terms of communications. Source: Internet Society

[3] In late 2011, first reports started to emerge that WCIT could become the forum for the most contentious international debate over Internet governance since 2005 when the process of the World Summit on the Information Society (WSIS) concluded.[3]

Dubai revealed (for example the discussion on how to deal with spam),[4] was that legitimate Internet concerns raised by nations, need to be addressed in appropriate venues; and that real solutions need to be identified otherwise they will continue to surface and become politicized. Hence, figuring out what the appropriate forum for such discussions will be is key to US positioning. In addition, the current lack of indigenous industry, experts, and civil society entities associated with the Internet in developing countries may continue to encourage the current focus on sovereignty and control. If industry is regarded as US or purely Western, the existing multi-stakeholder model will continue to be perceived a way to increase its influence. Supporting the emergence of national expertise in developing countries in particular through targeted capacity building can help build and maintain effective systems and build confidence in non-governmental players. It can also help level the playing field, ensuring that developing nations are better positioned to participate directly or indirectly (through trusted experts) in highly technical Internet governance fora.

- Despite these developments within the WCIT, another speaker asserted that Internet governance would not be determined in international fora, but rather in those countries where the population has most to lose from not having access to the Internet. Current demographics[5] suggest that there is a huge impetus for the existing infrastructure to continue to evolve in places where the institutional framework that binds peoples' ambitions i.e. that keeps them from achieving what they want in life - is the most subject to change. Indeed, cyberspace gives a new opportunity to rewrite and renegotiate the social contract between societies and states.

- Speakers also noted the importance of developing a deeper understanding of the political economy of the Internet as a means to better understand the desire of some governments to control it. In this regard, it is important to recognize that fees derived from international telecommunications represent a significant percentage of government income in countries with few other resources, particularly in the global south. Basically, governments want to have control over cyberspace because they want benefit from it locally. This also explains why we are witnessing a 'nationalization' of the Internet, i.e. the creation of content that will be paid for within national boundaries. The latter is leading to the creation of a two-tier system of the Internet, which would allow governments to charge different tariffs for national and international content. These are factors that are often over-looked in discussions on Internet governance.

A new narrative or time for pragmatism?

- Regarding future steps, speakers suggested that if the US is to maintain its influence, a first step

[4] According to one participant, the spam provision negotiated and included in the ITRs – [Art. 41C *Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense*] - does little to resolve the problem. Rather than reducing spam, the provision implicates the Internet, and sanctions the blocking of unwanted content. It also encouraged nations who wanted language on spam to support the ITRs as a whole.

[5] Today about two thirds of the globe is connected to the Internet. There are more cell phones on the planet than human beings. Of the people connected; 2/3 are under the age of 35; and 50 percent are under the age of 25. These groups represent young adults on the cusp of entering their most productive years of life. They are the ones who have most to lose and most to gain by how the Internet is shaped. In addition, three out of every five Internet users are located in developing countries, many of which are deemed fragile. The US represents about 11 percent of the global Internet population; the Euro-Atlantic alliance about 30 percent. Internet usage will only continue to grow over the coming years, with some of the most expansion expected in Africa and Asia.

would be to acknowledge that it may no longer in fact, be able to set the narrative unilaterally. It will therefore have to determine how to shape the impact of greater government involvement to best serve US interests, ensuring that the imposition of national governments does not for example, affect global inter-operability and human rights. While these issues are already included in the US International Strategy for Cyberspace, it is unclear how the US intends to go about upholding them given the new realities of international politics. Capacity building may serve as an entry point but a much more strategic diplomatic effort is needed.

What Role for the UN and other International Organizations?

- Finally, most countries see the UN as the central institutions for the global debate on Internet governance. While the US and other countries can and will continue to object to the ITU being involved it will eventually have to manage the transition away from a US-centric Internet. In doing so, it can help define the role of the UN and other international fora in moving forward. In this regard, assessing international organizations, their intent and capability jointly with other member states can help determine which institutions are best suited to be involved on these issues.

2.2 The report of the UN Group of Governmental Experts (GGE) working under the auspices of the UN General Assembly (UNGA) First Committee on Disarmament, agreed to in June and presented to the UN Secretary-General at the annual UNGA session in September.[6]

- As noted in the roundtable session on cyber warfare, the 2013 report of the UN Group of Governmental Experts (GGE) opens the door to reshaping the legal and political landscape concerning international cybersecurity. Following several years of difficult negotiations, consensus was finally reached this year among the members of the group on the applicability of the UN Charter, international law and the principle of national sovereignty to cyberspace; and state responsibility is the same in the cyber domain as it is in the physical domain. These are significant achievements not least because the GGE process has faced important obstacles since Russia tabled the first Resolution in the UN General Assembly First Committee on Disarmament in 1998.[7] China agreed reluctantly with central provisions of the report, in particular the commitment to observe international law, yet at the same time, it was heavily engaged in the discussions, not least because these issues are important to the country.

- Core questions moving forward include how each of these points that have been agreed upon apply in practice. There is still no agreement internationally, as to what constitutes the use of force in cyberspace. Determining what constitutes an armed attack in cyberspace as well as when to use cyber capabilities in self defense (as per Art. 51 of the UN Charter), will be complex, in particular determining how the principles of necessity and proportionality apply. The same applies to the Laws of Armed Conflict (LOAC).

---

[6] The UNGGE was the third of its kind to be convened and consisted of representatives from 15 states including the US, China, Russia, France, the United Kingdom, India, Germany, and Japan. It is tied to the negotiations conducted under the in the UN General Assembly's First Committee which has been discussing information security – the US prefers to use the term cybersecurity – since 1998 after the Russian Federation first introduced a draft resolution on the issue.

[7] After a first GGE failed to produce a report in 2005, a second GGE produced a consensus report in 2010. The current report builds on the latter.

- Several speakers noted that it is also necessary to be more careful with the use of certain words in describing cyber-related incidents. Terms such as war and warfare are not useful, not least because they are not used in international law. Rather armed conflict, or use of force should be used, depending, of course, on the context.

- Participants discussed one tool that has proved useful for more focused discussion on these issues - the Tallinn Manual – which was launched this year. The Manual provides an overview of the international laws relevant for both the *ad bellum* UN Charter and *in bellum* armed conflict laws, determining how these laws might be applied to cyberspace. Not everyone agrees with some of the suggested rules outlined in the Manual, but it has brought the discussion regarding the applicability of international rules to cyberspace to another level.

- In this regard, speakers also discussed the likelihood that any armed conflict will be solely 'cyber' i.e. it is highly unlikely that a 'cyberwar' *per se* will ever occur and some reality needs to be injected into the manner in which certain incidents and their effects are being described.[8] Indeed, as has been the case cyber capabilities will continue to be deployed as an additional form of fire within the framework of a more conventional armed conflict (e.g. the 2008 conflict between Russia and Georgia), or in the form of weaponized code used as a covert tool of sabotage and aimed at creating strategic effects and attaining foreign policy goals (for example the use of Stuxnet to put a break on Iran's nuclear ambitions).

- Cyberspace is also increasingly being used to create information effects both in and outside the theatre of war (e.g. Hezbollah's strategic use of information against the IDF in the 2006 war). In other contexts (e.g. Syria today), cyberspace is being exploited for targeting[9] and for command and control (C2) purposes.

- The cost-benefit analysis of the different uses of cyberspace and cyber capabilities is of increasing interest to all countries. To the US (and the West in general) because of their significant battle weariness following a decade of military engagements in Iraq and Afghanistan, and their general reluctance to deploy troops to other theatres; as well as the belief by some that cyber attacks may be an attractive alternative. And to those actors who do not currently (and probably will never) have the same type of military capability as first world actors, because of their growing realization that they can achieve political goals and bolster their positions by acquiring and deploying capabilities that have near-kinetic effects.

- One speaker noted that in the future, self-restraint may play an important role in the deployment of weaponized code. Unique among all weapons systems, weaponized code can often be used only once. When used against a target, the weapon is effectively given away to the opponent – the code can be reused, repackaging it in different ways. Hence, the ability to use weaponized code is not the same thing as using firearms. Sound judgment is required to determine when it is used and against which opponent, which is probably why higher-level authorities are currently required to deploy it.[10] Notwithstanding, clarification regarding the international legal uses of

[8] For example, the campaign against Saudi Aramco did not stop the company's production and its systems were restored within two weeks. The recent attacks targeting US banks led to outages of 30-60 minutes with limited impact on users.
[9] The Syrian regime is reportedly targeting doctors' mobile phones to access lists of patients – people who have been shot, and who most likely belong to an armed group.
[10] Reference to PDD20

such capabilities for political or military purposes, (during peace or wartime) is still required.

- A new Group of Governmental Experts (GGE) will likely be established in 2014 to continue discussions on the issues that were agreed upon.[11] A framework for norms and standards has been set - this is the political underpinning that was needed to move forward not only on the political and military issues, but also the Internet governance ones. In this regard, the Snowden debacle might actually be beneficial to the international community and the US in the sense that it provides a window of opportunity to move forward on some of the more sensitive issues that were hampering progress on the international security front.

- Finally, and important to bear in mind regarding the new Group of Governmental Experts (GGE), is the fact that other, related issues are being increasingly discussed in the UN: the use of unmanned aerial vehicles (UAVs)/drones and robotic weapons all of which are controlled by or channeled through cyberspace. There is a very strong push to place these under international humanitarian law and the topic may be officially placed on the agenda next year, potentially representing a new frontier for cyberspace related discussions.

- Moving forward, speakers suggested that the US should develop a more coherent strategy. To date it has been speaking with two voices: one focused on a peaceful and stable cyberspace; and the other heavily focused on developing military and intelligence cyber capabilities or exploiting cyberspace for political or strategic effect, thus sending confusing signals to other countries.

2.3 Edward Snowden's intelligence disclosures and other forms of espionage

- Obviously nobody was prepared when on June 5, 2013, the UK-based newspaper *The Guardian* published its first in a series of articles based on revelations by Edward Snowden exposing the surveillance systems operated by a variety of states, particularly the US, via the National Security Agency (NSA) and the UK, via Government Communications Headquarters (GCHQ). On the one hand the Snowden revelations have provoked much ire among many of the US's traditional allies as well as those the US was hoping it could sway on the Internet governance and norms agendas.[12] On the other hand, other states have taken note of the capabilities and are seeking to emulate them or join the countries that most benefit from them.

- As noted by the speakers in this session, the full ramifications of the Snowden disclosures remain unknown at this point. They have however, demonstrated how intelligence agencies operate, and that they will make full use of new technologies as they become available, just as they did after the 9/11 terrorist attacks. Moreover, regardless of the point that some leaders are making about spying being a normal feature of international relations, it is unclear what the grand strategy underpinning the scale of espionage the US has engaged in actually is. Counter-terrorism alone cannot be the justification nor can the reasoning that the US uses these capabilities just because it has them and can use them. This raises the concern that the intelligence agencies' risk-benefit analysis has been skewed, that they have become too big and

[11] Russia tabled a Resolution during this year's UNGA session calling for the establishment of a new GGE in 2014 to continue discussions on these issues. Member states have agreed to this proposal and discussions are on-going to determine when exactly this might happen and what the composition will be, whether 15 members as is generally the case, or an expanded group of 20.

[12] For example, Brazil and Germany tabled a Resolution on privacy issues during the UN General Assembly; and Brazil has also approached India to organize a global summit on US surveillance in 2014.

unmanageable, and that this reality needs to be adjusted before something really serious occurs.

- Participants discussed their belief that the US National Security Agency (NSA) had hacked US companies, allegedly without their knowledge, and the benefits and risks of inserting backdoors in software and hardware. Speakers also highlighted that international law does not govern espionage and that there are no instances in which espionage activity has led to war.

- In moving forward, it is evident that trust between nations and between governments and civilians needs to be restored. Issues pertaining to surveillance, privacy, Internet governance and cybersecurity are constantly overlapping and unless there is some trust injected into these activities and processes, there is an extraordinarily high probability that national governments will impose measures affecting the Internet as we know it with serious consequences for economic development and human rights. Questions abound regarding whether vulnerabilities should be disclosed to the public so they can be patched, or whether they should be kept as a state secret for espionage or warfare.

- Domestically, speakers remarked upon the fact that the Snowden revelations have invigorated the existing focus on privacy issues. Several bills, including the Cybersecurity Information Sharing and Protection Act advanced by Congressmen Mike Rogers and Dutch Puppersberger have been tabled in Congress. The Snowden revelations have only served to stall discussions on the different bills. Yet, questions abound regarding the influence that certain technology and content-oriented companies currently have on lawmakers in Washington D.C. Conversely, if California is anything to go by, the US already has a *de facto* privacy policy since whatever is happening in California tends to become a *de facto* privacy rule. Indeed, to date, some 16 bills on privacy have been introduced in California.

- Beyond the Snowden revelations, the point was also made that the current focus on the NSA surveillance issues has shifted focus away from other core issues, particularly the allegations of Chinese cyber industrial espionage. Indeed, the diplomatic strategy that the US administration had developed over the past year to address the issue was essentially put on hold by the Snowden revelations. During the previous months, the US government had built up significant pressure through a series of speeches by senior government officials further substantiated by internal intelligence and industry reports.[13]

- Finally, as suggested by several speakers, norms for responsible behavior in and with regard to cyberspace are shaped by action. Yet, current actions are undermining the US' legitimacy to lead. In this regard, the US should revert to its strategy of agreeing on what is acceptable state behavior when it comes to espionage, and highlighting common problems as a means to convince the Chinese government that it is in its own interest to engage with the US (and other nations) on cyber industrial espionage-related issues.

[13] For example, Mandiant's "Advanced Persistent Threat" report published in X.

3. What next for US Foreign Policy?

- Discussions on developments in the three core areas – Internet governance, cyber war/ conflict and espionage - highlighted in the previous section demonstrated that there is an emerging international consensus with regard to the applicability of the UN Charter, international law, the laws of armed conflict and principles of sovereignty and state responsibility to cyberspace, and a convergence of the Internet governance and cybersecurity fields.

- Many of the challenges discussed revolve around political differences between states, for which political solutions must be sought through a more pragmatic and targeted foreign policy. If anything, the revelations reinforce the argument that global [cyberspace] infrastructure that we (and the global economy) depend on is not secure and is not securable through technological means, hence political understandings are needed in order to provide a more stable environment.

- Concurrently, and as suggested by several speakers, a more targeted US foreign policy needs to also consider some glaring realities in the global strategic environment, which are briefly discussed below.

Competing Values and Interests

- As noted throughout the meeting, the US is less influential today than it was in the 1990s. Indeed, the old way of thinking is facing serious challenges, particularly some of the democratic ideas that have shaped how we think about the Internet. For example, in the 1990s, much attention was afforded to underpinning policy with important value-laden theories, with the end of the Cold War representing "the end of history," a lesser role for governments, the mushrooming of market economies and so forth.

- When China and Russia entered the western community and became market economies, there was an erroneous assumption that they had taken on Western values. Yet, they continue to question some of the fundamental assumptions it was assumed they would endorse despite the number of tools and mechanisms that have been developed internationally to spread them. Consequently, very different concepts about how the Internet should work and what the rights and obligations of states and citizens are vis-à-vis cyberspace have emerged. In this regard, the geo-political landscape can be split into several camps:

    - The first group, Western countries, is committed to the status quo and refuses to recognize in large part that the status quo is changing. The West also has a strong view on the importance of non-state actors. Many other countries do not share this view particularly with regard to private sector and civil society and their participation in different processes. This may be a bone of contention in the future.
    - The second group of governments, especially countries in the Arab region, views cyberspace as a threat and would make it go away if they could.
    - A third group, namely Russia and China, is concerned about issues of disorder and committed to controlling political discourse. They are also concerned with securing capabilities that will bolster their strategic posture and help them attain their strategic

interests.
    - Another set of countries such as India, Brazil, and South Africa expect that they deserve a more substantial role due to their growing influence in the world. These countries have traditionally also been very active in taking issues to the UN.
    - A fifth group of countries, primarily in Sub-Saharan Africa, that is seeking access to the infrastructure and some of the rents that can be extracted from content.

Transformation in the Character of Warfare

- As noted at the outset, significant transformations in the character of warfare are taking place in part due to the overwhelming imbalances in conventional military capabilities of some countries (mainly the US) vis-à-vis others; and in part due to the desire of the US to disentangle itself from the theatres it has been militarily engaged in over the past decade; as well as a realization of the geo-strategic importance of Asia to which the US has turned its attention. In this regard, efforts to use cyber capabilities (either as a form of fire, or by using information to affect outcomes) or cyber-guided technologies such as UAVs, to advance certain foreign policy goals and/ or create strategic effect has become more pronounced.

- While some of these uses of cyberspace and cyber capabilities might have stoked distrust among nations, their effectiveness in producing near-kinetic effects has also provoked a race between states to emulate or acquire them, thus placing additional pressure on the international system and the institutions and mechanisms responsible for managing international peace and security.

- Looking further ahead into the future of armed conflict and the place of cyberspace and its uses in armed conflict, there is also a need to take into account trends that have been obvious since the 1990s including the declining rate of interstate war, the increasing rate of intrastate conflict, as well as an increase in a range of conflicts that take place in urban settings.[14]

Is a New Policy Approach Required?

As noted during the meeting, the current US strategy for cyberspace is centered on:

i. *A military strategy* for cyberspace which to date has been largely successful in developing cyber capabilities and military doctrine (some of which have been disclosed by *The Guardian*), but highly criticized by some observers.

ii. *A diplomatic strategy*, which unfortunately has not always been obvious. The thrust of the diplomatic strategy is to work closely with the United Kingdom and other like-minded countries to make cyberspace more stable and secure by defining responsible state behavior. The diplomatic strategy will face more complex challenges because of the Snowden revelations; yet if the progress made to date within the UN GGE, the OSCE, the ARF, and the Seoul Conference is considered, overall the strategy is producing

[14] See David Kilcullen, *Out of the Mountains,* in which he discussed mega-cities; littoral cities and highly densely connected cities where the ICT environment is integrated within the fabric of society and where using conventional military force or even COIN approaches will no longer be an option.

positive results. While the goals of this strategy remain valid, it will need adjustment.

iii. *A strategy to secure the US (infrastructure).* This dimension of the overall strategy has not been successful particularly if we consider that we are no more resistant to attack than we were five years ago. This is a symptom of the larger political problems the US is facing.

Assessing what the current cyberspace strategy has achieved against some of the core achievements and setbacks of 2013 and the shifting global strategic environment is necessary to inform the future direction of US foreign policy in this area. Indeed, as suggested by participants, there is a need for fresh thinking and a new narrative that recognizes some of these core developments; and defines where the US stands, and where it wants to go in relation to them.

5. Policy Recommendations

The latter presents a number of questions that policymakers in particular, need to explore in the coming period:

- What will US foreign policy look like after a decade of war, bearing in mind the changing character of war and how cyber capabilities are being used to affect political change both in and outside theatres of war? And how do we put cybersecurity in the context of global political change, which is what we are seeing?

- What are the tools and concepts of that foreign policy?

- How do we deal with the reassertion of sovereignty over cyberspace by other countries and the fact that it has now been agreed upon within the UNGGE? What are the real contests that will affect both democratic values and the US economy in the coming period?

- What outcomes should guide the foreign policy debate? What trade-offs need to be assessed? For example, how much do we want to protect the current Internet governance model which is US centric and very favorable to the US; and how much do we want to make concessions that may reduce in some ways the advantages the US has had, but is more in tune with political economy realities of other countries and might produce a more stable environment.

- What are the vehicles for collective action for international security? Is it the UN or other? How can the US help build collective action, and how much influence does the US have left to do so? How well do existing rules and institutions work. Existing laws and institutions are relatively weak, the former are not clearly understood and sometimes the rules might be unspoken. Hence, understanding how well they work would help determine the changes that are needed.

- Can we develop a new road map for dealing with espionage? How are the Snowden revelations affecting bi-lateral discussions with Russia and China? How are they affecting the transatlantic relationship? How can we manage existing cyber industrial espionage challenges

while dealing with the spillover effects of the Snowden revelations?

- Digital trade and cross border data flows. The latter will continue to be a big issue for the transatlantic trade talks. What is digital trade? What do we do with cross-border flows? How do we deal with the push to control data storage and prevent economic damage nationally (because we occupy so much of the space), but also globally?

- How can the current interest in capacity building be more effectively targeted at some of the states that have legitimate concerns and needs?

The NCAFP will address some of the questions raised and recommendations made in the report over the next twelve months and will continue working with a wide range of experts to engage in policy-relevant cybersecurity discussions with its members and the broader public.

Camino Kavanagh[15]
22 November 2013

[15] The summary report was crafted with significant input from Tim Maurer who served as rapporteur during the meeting; Edythe Holbrook and Elena Garofalo. The NCAFP team is also grateful to Dr. James Lewis for his invaluable insights and suggestions.