Cybersecurity, Sovereignty and U.S. Foreign Policy

21st Century Leaders Council

2014 Cybersecurity Roundtable

(with NCAFP Policy Recommendations)

New York City

Tuesday, November 4, 2014

Our Mission

The National Committee on American Foreign Policy (NCAFP) was founded in 1974 by Professor Hans J. Morgenthau and others. It is a nonprofit activist think tank dedicated to the resolution of conflicts that threaten U.S. interests. Toward that end, the NCAFP identifies, articulates, and helps advance American foreign policy interests from a nonpartisan perspective within the framework of political realism.

American foreign policy interests include:

- preserving and strengthening national security;
- supporting countries committed to the values and the practice of political, religious, and cultural pluralism;
- improving U.S. relations with the developed and developing worlds;
- advancing human rights;
- encouraging realistic arms control agreements;
- curbing the proliferation of nuclear and other unconventional weapons;
- promoting an open and global economy.

An important part of the activity of the NCAFP is Track I½ and Track II diplomacy. Such closed-door and off-the-record endeavors provide unique opportunities for senior U.S. and foreign officials, think tank experts, and scholars to engage in discussions designed to defuse conflict, build confidence, and resolve problems.

Believing that an informed public is vital to a democratic society, the National Committee offers educational programs that address security challenges facing the United States and publishes a variety of publications, including its bimonthly journal, *American Foreign Policy Interests*, that present keen analyses of all aspects of American foreign policy.

CONTENTS

INTRODUCTION

Camino Kavanagh and John B. Sheldon

The topic of this year's cybersecurity Roundtable meeting was *"Cybersecurity, Sovereignty and U.S. Foreign Policy."* It was held in tandem with the publication of a series of articles on the same topic in the National Committee's journal, American Foreign Policy Interests.

Why, might you ask, the focus on cybersecurity, sovereignty and U.S. foreign policy? In the 1990s, many premised that the advent of the information age would lead to the demise of the nation-state through the erosion of state power and, as a result, state sovereignty. Moreover, the Internet and a space many today call "cyber" would enable the emergence of the sovereign citizen, free of the political, economic, and security demands of the all-powerful state. Yet, such predictions not only did not transpire; they became the poster child of the old adage "be careful what you wish for" in today's age of global terrorism and sophisticated organized criminal activity. In hindsight, the assumption that the information age would somehow transmute the human condition seems rather naïve.

Certainly cyberspace has empowered individuals around the world, for both good and bad. Yet, it has also given states a new domain or environment in which to expand their power and in which to compete with one another. State sovereignty, while far from undermined, today boasts a more porous character reminiscent of the eighteenth and nineteenth centuries, when states were certainly the most powerful actors on the international stage but not the only actors with influence. As the malicious uses of information technologies and cyberspace continue to disrupt social and economic institutions, how states assert their sovereignty and compete with one another will continue to change and adapt as will the role of individuals and private organizations and actors as they compete for space on the international stage. Through its three core sessions, the 2014 Roundtable explores many of these dynamics and interplays, highlighting pending policy dilemmas or putting forward a series of recommendations about the future direction of U.S. foreign policy and strategy in this area.

The first panel, moderated by **Melissa E. Hathaway**, frames the problem through the lens of a number of sovereign dilemmas that policymakers face today. A core question debated during the panel and throughout the day centered on whether the current U.S. strategy is sufficient to handle the multiple challenges at hand and whether the links with broader U.S. foreign policy are tight enough.

The second panel, moderated by **Rafal Rohozinski**, focused on changes in military affairs, questioning whether it is possible to fit today's cyber and information warfare capabilities into traditional military constructs and doctrine, and how they these changes might affect the future character of warfare. The use of special forces for an ever-widening range of operations is used as a case study, fitting into a wider debate in the U.S. national security community about the future of warfare and whether what we are experiencing is a new revolution in military affairs (RMA).

Moderated by **Dr. Roger Hurwitz,** the third and final panel provided an extensive overview of the current norms environment: What norms actually are, how they relate to cyberspace and cybersecurity, who decides on them, how we implement them and so forth. Efforts by the U.S. government in this area are showcased in this panel—as are those of academia and the private sector. The core questions raised in the panel include how we move from the current cacophonous normative environment to one in which objectives and roles are more evident, and how progress against bigger-picture foreign policy issues can be assessed.

Finally, as with last year's Roundtable, a recurring theme throughout the meeting related to whether the U.S. government and U.S. information and communications technology (ICT) providers can influence outcomes in a shifting and complex global geopolitical environment in which normative disintegration and disengagement are increasing and in which the United States itself has undermined some of the normative values it is hoping to promote and project into cyberspace and the Internet. Again this year, it is a question that remains unanswered, but one that requires serious deliberation.

SUMMARY OF DISCUSSIONS

Panel 1
Connected Choices: The Internet and Sovereign Decision Making

Framing the Problem

Moderated by Melissa E. Hathaway, the panel kicked off with an introduction to the history of the Internet from its inception in 1969 as means of transmitting data between two universities through its strategic inflection point in the late 1980s–early 1990s with the advent of e-commerce and enhanced military and civilian uses to today with every service in modern societies connected to the Internet. In this regard, increased connectivity has become part of the transformation or development agenda of every country around the world.[1] In developed countries, participation is no longer opt-in, but rather compulsory since almost everything we do is contingent on connectivity, i.e., it is now the system necessary to participate in society.

Building on an essay she wrote for NCAFP's journal *American Foreign Policy Interests* on the same topic,[2] the moderator addressed the range of Internet-related vulnerabilities the United States is facing today from the perspectives of economic, technical, regulatory, political, and social interests. She placed these challenges within the broader challenge of "multicultural friction" revolving around the realities of digital destruction (Stuxnet 2010), digital diplomacy and discord (WCIT, Dubai 2012), digital defiance (Snowden revelations 2013), and digital dependence (40% of the world's population connected to the Internet in 2014).

Homing in on the question of national sovereignty, panelists noted that there is a clear drive by some states to reassert their sovereignty over many aspects of cyberspace. Many of the issues we are currently dealing with have direct implications for national sovereignty, but others less so, particularly because of their transnational or universal/transcendental character. The latter clearly include the freedoms and rights generally associated with the U.S. Bill of Rights, as well as open trade, competition and innovation, and cybersecurity itself. Another of the panelists insisted on the need to view the Internet from the perspective of a multilayered global communications network: its land and undersea cable networks telecommunications carriers, the protocols and governance of domain names and numbers, the definition of software and hardware, etc. The underlying infrastructure—for example, undersea cables and their landing stations—is particularly vulnerable.[3] Enhancing protection of the

undersea structure and reducing the time required to repair damaged cables should thus be major priorities.

To make sense of these intermingling ideas of sovereignty and transnationality, one of the panelists proposed assessing them from six different yet interrelated perspectives: cultural sovereignty; geographic sovereignty; data sovereignty; cybersecurity; human rights; and economic security. The issue of data sovereignty in particular was emphasized in light of recent efforts by some countries or regional groupings to protect data from external surveillance and keep citizens' data within territorial boundaries. Such steps, panelists surmised, would have serious implications for current trends in data storage and for international commerce in general.[4]

The fact is that we are dealing with a tremendously complex system that, by definition, is unmanageable despite efforts to bring it under some form of formal governance structure. Rules can indeed be assigned to the system, but a more effective approach would be to avoid heavy regulation. Nonetheless, this very issue is driving serious competition between states. For the moderator, the current push and pull between states regarding cyberspace, particularly ongoing debates and processes surrounding Internet governance, is part of a broader strategic, multidimensional competition for money, power, and control over all aspects of the Internet and the Internet economy. With technological advantage at the core of any major power's strategic posture, she cautioned that only those states that understand this multifaceted environment and are willing to make the right investment of resources and manpower will "end up on top."

In terms of U.S. response to these issues, the panelists largely agreed that the current approach is insufficient. In this regard, the United States requires a much bolder strategy and a much bolder foreign policy to link it to. A simple narrative defining where we want to go and how to go about it would suffice. At present, however, the government does not appear to have a coherent strategy or any defined "end game" or vision for the Internet and cyberspace around which the various government entities can coalesce or around which to work with allies or like-minded nations. This situation has only become more acute following the Snowden revelations, exacerbating existing tendencies to view many of these issues from an East-West or developed vs. developing nation perspective. It is a key area of U.S. foreign policy and thus requires serious consideration.

In response to these assertions, some participants insisted the contrary: that the United States does have a strategy—the 2011 U.S. International Strategy on Cyberspace—which forms a core part of

the administration's foreign policy and that a coherent vision exists across sectors (for more detail, see Panel 3 below).

Pending Policy Issues

Moving forward, panelists and participants slated a number of questions:

- How can current policy and strategy allay concerns regarding the fact that the Internet is a U.S. creation upon which the entire world is becoming increasingly dependent, thus posing a serious national security challenge for a number of states, including many allies and particularly following the Snowden revelations?

- The process whereby some states are asserting sovereignty over the system's infrastructure is a natural one. Yet, what should the response be regarding this process, particularly when it affects content? Do we need to invigorate our current position on these issues or review it?

- Much of the discussion on Internet governance at present is related to the Internet as we currently know it. Yet, it is bound to change. What might the Internet look like in the future, for example, some 20 years from now? And what modes of governance or management might that future Internet require? Also, how will future policy and strategy consider a different geopolitical context in which the United States is no longer the preeminent world power? And is the United States prepared for the eventuality of a new Internet governance model emerging from ongoing discussions within the International Telecommunications Union (ITU) or other fora?

- How will the tensions and trade-offs between security and privacy be reconciled given the increase in terrorist and organized crime activity on the Internet?

❖

Panel 2
Information/Cyber Warfare and Territorial Sovereignty: The End of Defense?

Moderated by Rafal Rohozinski of the Canadian group SecDev, Panel 2 focused on discussing cyberspace and the changing character of warfare and what this means specifically for the age-old concept of defense, a bastion of the territorial sovereign state. The panel discussed the challenges posed by the fact that national defense is no

longer just defense against peer nation-states (as has been clear for more than two decades now) and that defense does not begin or end with national borders. The Islamic State's (IS) use of social media for global recruitment, financing, and command and control purposes is a case in point. That the group is openly using social media for these purposes poses huge challenges to national security agencies and private tech companies at a time when the debate on National Security Agency (NSA) powers vis-à-vis privacy rights is at an all-time high. What remains unclear is how these tensions between security, defense, and privacy will be resolved.

2.1. Special Operations Forces: What Shoe Do They Fit?

In addition, the moderator and panelists discussed new trends in cyber and information warfare, questioning whether the current emphasis on reaching agreement on norms to shape state behavior and as a means to achieve stability in cyberspace is suited to the actual operational environment. According to the panelists, these kinds of norm-setting efforts have rarely taken into consideration the fact that today most conflicts, which increasingly involve the use of cyber capabilities (i.e., weaponized code) or information, warfare are seldom declared and that the use of force (still largely undefined in this area) occurs under a number of executive titles and authorities and is increasingly implemented by special forces.

For example, the panel discussed how recent events in Ukraine and elsewhere demonstrate how tactical uses of cyber/information warfare (IW) capabilities are critical to special force operations—and not just those of the United States.[5] In this regard, even what might be viewed as traditional intelligence operations implemented under intelligence authorities look more like special forces operations, with Operation Olympic Games (more commonly known as Stuxnet) being a possible case in point. Arguably, cyber capabilities and special operations forces go hand in hand—many of the requisites of special forces operations, such as speed, agility, stealth, force of action,[6] are dependent on an operating environment where intelligence is paramount and operations security must be preserved. Therefore, understanding cyberspace and the multifold uses of ICTs is key for the intelligence preparation of the operational battle space. It is also key for targeting purposes, for operations security,[7] and for achieving the shaping effects required both for the insertion of special forces and the successful implementation of operations. In this sense, perhaps it would be more useful to view cyber capabilities more as "employable capabilities" within the framework of special forces operations rather than how we have been framing them to date, i.e., as a strategic capability.

Related to the discussion of cyber (or weaponized code) as an "employable capability," participants also discussed the challenges of applying traditional arms control constructs to such capabilities—not least because of the challenges such efforts might pose to broader questions of interoperability and free flow of information. Yet, as noted by one of the participants, some progress has been made at least in terms of mitigating the export of surveillance technologies (for their use, for example, by authoritarian governments) through the Wassenaar Arrangement's[8] agreement in December 2013 to include changes establishing new controls relating to intrusion software and Internet Protocol (IP) network surveillance systems.[9] The question however, remains whether these changes will be applicable to the world we are moving toward, not least because not every country or company shares the same values.

2.2 The Transition

Within a broader discussion on the transition the international system is currently undergoing—i.e., from the unipolar, post–cold war order premised on liberal democratic ideals to a multipolar one in which these ideals are increasingly contested and where deception and opaqueness figure significantly—panelists questioned the capacity of the state-based international system to respond to today's challenges. In the past, we have persistently established institutions to deal with all the uncertainties prevalent in the international system, yet with these changes in scale, proximity, and precision driven by developments in the sphere of information technology, we have helped undermine the international system's presumptions about conflict. Furthermore, it will be possible to establish borders in cyberspace over time—some countries are already doing so. In this regard, one of the panelists suggested that our current notion of territorial borders would eventually be overtaken by a form of "cyber Westphalia" in which information flows will be highly unpredictable, with deep implications across sectors.[10]

In this regard, states, while still core actors, are not the only ones. Cyberspace, a man-made complex system perhaps better understood as a substrate of existing domains (land, air, sea, and space), is, in part, driving the transition the international system is undergoing, particularly if considered from the perspectives of scale, proximity, and precision.[11] It is precisely these issues that we need to bear in mind when thinking about strategy and warfare moving forward.

2.3 A Revolution in Military Affairs?

Discussions also focused on how the use of special forces for an ever-widening range of operations is part of a wider debate in the U.S.

national security community about the future of warfare and whether what we are experiencing is a new revolution in military affairs (RMA). Some participants cautioned that it will be important not to overreact to current developments in the field of information technology, since what we are ultimately witnessing is an adaptation of warfare (as well as the human condition) to these developments as well as new circumstances. Moreover, over-emphasizing the power of cyber capabilities in warfare (as some have done by suggesting a revolution in cyber affairs) might lead us down the same dangerous path blazed by RMA-evangelists in the 1990s—the one that obviated politics and the human dimension altogether.

2.4 Pending Policy Issues

Key questions remain however. For example:

- If we accept the proposition that ICTs are an employable military capability, what does this represent? Something revolutionary, i.e., does it force us to redefine how we look at national security and national defense? Or is it evolutionary, i.e., more of the same with different characteristics? Or both evolutionary and revolutionary? If so, what does this represent for the way the military is currently organized?

- More specifically, how can national security and national defense postures adapt to the dynamic character of warfare today, especially given their objective of protecting key strategic interests, but also given i) existing and emerging political and legal norms aimed at placing limitations on states' exercise of cyber power and ii) the geopolitical shifts we are currently witnessing in which the United States is no longer the sole global power?

- More specifically, how can we frame cyber/information warfare operations in this shifting context? Do they fall more appropriately within the realm of hybrid or unconventional warfare? Under law enforcement operations? Should they be dealt with on a case-by-case basis as suggested by one of the panelists?

- In this regard, is the current focus on taming cyber power through the application of existing or new norms, including the laws of armed conflict, erroneous? What are the alternatives? Is it possible to take a two-pronged approach? One aimed at shaping state behavior regarding the uses of cyber capabilities and cyberspace at the strategic level; the other ensuring that tactical uses of cyber capabilities (i.e., weaponized code) for operations other than war are framed through policies and authorities in a manner that

protects basic rights and establishes inter alia clear command and control duties and responsibilities?

- To what extent can discussions on the use of cyber capabilities be linked to ongoing discussions on the weaponization of automized technologies/robotics?[12] For now, these discussions seem to be completely siloed, with limited participation of experts across thematic areas. Can lessons be shared across these thematic areas?

- What are the national security implications of our increasing reliance on special forces (including specialized units with enhanced cyber and autonomous capabilities) for tactical purposes (i.e., as employable capability) in foreign theaters where we are not at war in the traditional sense?

- What challenges or opportunities does the deployment of special forces represent for the exercise of other instruments of national power and for ensuring stability in the international system?

- What are the implications of the deployment of special operations forces on state-society relations?

Panel 3

The Play of States: Norms and Security in Cyberspace

Panel 3, moderated by Dr. Roger Hurwitz and building on the essay he penned under the same title for *American Foreign Policy Interests*,[13] discussed how the norms of cyberspace that seemingly held two decades ago have been outmoded by the Internet's own success—a thousandfold growth in users across the globe and millions of applications. The fabrics of our individual and collective lives have become digital. The use of digital networks to manage and integrate information, transactions, and infrastructure has grown so pervasive and complex that the dependencies among them and our dependence on them might only be known if they unraveled. For the moderator, these changes have created opportunities for state, non-state actors, ephemeral groups suddenly empowered through social media, and even individuals to do perhaps as much mischief as good in cyberspace. Terms like *cyber crime*, *cyber warfare*, *cyber Pearl Harbor*, or *cyber terrorism* have pitched us against an ocean of uncertainty and instability.

The legacy of the Edward Snowden revelations still reverberates; states are openly at odds on what the lines for appropriate behavior are; the challenges industry faces are well-documented; and the robust markets—black, white, or gray—for buying and selling malware are thriving—and we seem to be witnessing a normalization of cyber *in*security. Yet, despite a common sense of vulnerability and many discussions on the need for new norms, states and other relevant actors have reached, at best, limited agreement on what norms should apply. With this background in mind, the panel discussed current efforts by states and other actors such as transnational companies and groups in civil society to define and promote norms, the strategies and frameworks for these efforts, and the obstacles they encounter.

3.1. Cacophony or Concert? Thinking About Norms in the Context of Cyberspace and Cybersecurity

Many of the aforementioned efforts were captured in a detailed overview of the current norm environment described as neither "cacophony nor concert."[14] In accordance with the standard definition, a norm is a collective expectation for the proper behavior of actors with a given identity.[15] This definition can be broken down into four core elements: identity, behavior, propriety, and collective expectations. In cyberspace, each of these elements exhibits a broad range of candidates that, taken together, produce the cacophony image.

- **Identity** Who do the norms apply to? At present, a broad number of cybersecurity norm entrepreneurs exist, with little consensus on which deserve attention or how to prioritize them. States are the most obvious community to which the norms apply. Efforts like the 2012 World Congress on Information Technology (WCIT) regarding Internet governance or the ongoing talks within the framework of the UN Group of Governmental Experts (GGE) aim to do this. Different groups of states can form smaller communities around regional affiliations, like-minded groupings or membership in international organizations like NATO or the OECD. The important point to bear in mind is that states are not the only entities that matter in cyberspace. Dozens of other groups can either shape or be the object of cyber norms. For example, the Budapest (Council of Europe) Convention on Cybercrime is aimed at developing norms to shape or mitigate the behavior of non-state actors—individuals, criminals and criminal organizations, etc. Industry affiliations play a role in shaping cyber-security norms. These include, for example: Internet Service Providers (ISPs), the undersea cable community, those companies involved in the manufacture of hardware, software, or critical infrastructure (for

example, the National Institute of Standards and Technology [NIST] cybersecurity framework).[16] White-hat groupings such as Community Emergency Response Teams (CERTS) also develop norms, so, too, do black hat groupings (e.g., Anonymous). Even victims as a group can be subject to cybersecurity norms in terms of expectations about certain types of behavior, for example, disclosure of data breaches as the Securities and Exchanges Commission (SEC) currently requires for certain publicly traded U.S. companies. This list does not even touch on the array of multi-stakeholder groups, affiliations, and associations that stress the importance of universal norms and their applicability to cyberspace.

- **Behavior** This is the functional element of norms aimed at prohibiting certain actions, encouraging specific behavior, etc., at varying levels of specificity. When thinking of behavior, we generally think of norms that proscribe behavior. This is the essential function of rules on crime or warfare. Cybersecurity norms can also dictate what states or other actors have to do, for example, the duty to assist in the face of cybersecurity threats.[17] There may also be norms that empower actors or encourage behavior—a point that scholars such as Jonathan Zittrain argue is fundamental to the generative nature of the Internet. Beyond determining which kind of behavior should be regulated is the level of specificity at which we regulate. Some norms are very specific. For example, the norm that now favors using Unicode character sets, encoding HTML since it includes every language in contrast to the prior English-only standard of ASCII. It is important to assess this variation of specificity and how it affects behavior.

- **Propriety** This is the core of the norm concept in that there is something out there on which we base the expectation of behavior—the permissible and the impermissible. The basis of the norm can be legal or political or cultural. Domestic law, for example, offers a range of norms from cyber crime to cybersecurity. Examples include India's law on authorized access; China's legal requirements obliging users to accept government supervision of their use of the Internet. In international law, the *Tallinn Manual* seeks to elaborate international legal norms applicable to cyber warfare.[18] At the same time, international law in this area is not all about warfare. Legal norms and regimes also emerge in relation to international trade, international telecommunications, or human rights—for example, the UN General Assembly's recent Resolution on the Right to Privacy[19] or the European Court of Justice's recent articulation of "a right to be forgotten."[20] As noted, political processes also form the basis of norms, many of which are

state-centric, for example, the London process on cyberspace; the OSCE's 2013 parliamentary declaration and resolution on cybersecurity and confidence-building measures (CBMS); or the 2011 Russia-China proposal for an International Code of Conduct for Information Security. Other international processes involve non-state actors, for example, the Global Commission on Internet governance (also known as the Bildt Commission)[21] the tech grouping that led to the Montevideo Statement on the Future of Internet institutions.[22] Regarding cultural norms, these can emerge from participation in a specific community. For example, the Internet Engineering Task Force (IETF) or ICANN have become acculturated, setting out expectations of behavior. Other technical communities such as international humanitarian lawyers, intellectual property experts, or even the cyber-security community share that approach. Finally, we should not forget Lawrence Lessing's lesson that "code is law," i.e., that how the technology's architecture is set up has normative implications in the sense that it affects what we can or cannot do on the Internet.

- **Collective expectations** This is the existential element of a norm, the concept that the norm involves some form of shared consciousness or unconsciousness; the belief in the norm's existence and that behavior will be expected to occur not just now, but going forward. This is the area in which most disagreement has emerged to date. Today, it is often hard to determine when and where actions or inactions are the product of a shared collective expectation of a cybersecurity norm. Even if we think that something might be related to a specific norm, the tools to contextualize it (i.e., when, where, how the norm will operate in a world of so many other norms), are limited. What also remains unclear is which of the norms are default norms and which are peremptory (i.e., the norms we are not supposed to violate); how we should relate norms to one another; which should be prioritized; and which should fall away.

This overview demonstrates the current level of cacophony within the concept of cybersecurity norms itself, but that current cacophony is also evident at the next level up—i.e., the norms on norms, the secondary rules involving the "who decides who decides" question. The norms on norms in cyberspace are highly contested, most obviously in debates over Internet governance—with some arguing that the Internet should be controlled like other IT resources in the past and others who stress a more bottom-up approach. Both camps presume that some authority or process can dictate norm formation, but it is precisely here where the sociological aspect comes to bear,

that is to say, this is not how norms always work. They are not always so neat. Certainly, some authority can dictate them, but they can also emerge organically over long periods of time without any clear sense of why. In between are a great number of norm entrepreneurs who want to break the status quo and change things, but there is limited consensus as to who should get a fair hearing and which entrepreneur we should listen to and which we should ignore.

The combination of these factors, i.e., the variation in norms in terms of identity, behavior, propriety, collective expectations and the norms on norms question, is what gives the impression of a cacophonous environment, posing serious theoretical challenges for arriving at what might be called a "concert"—a more harmonious environment. As was obvious throughout the meeting, serious issues remain unresolved and important questions unanswered—for example, the discussion on the *stewards* vs. the *sovereigntists*,[23] in turn linked to the discussion on how to define or characterize what cyberspace actually *is* and what it is *for* (for the overall good of society vs. the security of the state). The absence of mechanisms for sorting out behaviors or theories for resolving conflicts among norms for cyberspace poses important challenges for prioritization in policy.

Despite the manifold challenges, the panel discussion focused on how, moving forward, normative progress might be made in three specific areas:

- **Consolidation** The process of dictating norms is going to have to consolidate sometime soon. We are in the year of infinite meetings: At some point, the transaction costs will narrow down the list of where and when these conversations on norms are held.

- **Incompletely theorized agreements** There is the possibility that we might get to some form of global midlevel cyber norms even if we cannot agree on what cyberspace is for or what it is. Cass Sunstein's theory of "incompletely theorized agreements" can help us understand what this means, i.e., we can, at minimum, agree on something being good or bad, something we should do or not do, even if we don't agree on the why.[24]

- **Siloing** In certain areas, we are already seeing a degree of siloing, for example, through the 2013 changes to the Wassenaar Arrangement, the *Tallinn Manual*, etc. A next step might involve groups of states moving beyond discussing whether X or Y is a norm to discussing how to contextualize it: What it means, how to prioritize it, etc. Maturation of norms might also become evident

in some areas, for example, international telecommunications or human rights regarding cyberspace, security, etc. The challenge, however, is that there are limited mechanisms for cross-silo talk that could, in turn, pose additional problems if decisions are made about norms in one area without regard for how such decisions will impact other areas.

3.2. The Government Response: Give Strategy a Chance!

In response to some of the assertions tabled in Panels 1 and 2 regarding the existence of, the effectiveness of the U.S. government's foreign policy and strategy for cyberspace, and the deployment of cyber capabilities, the government representative on the panel provided a detailed overview of government efforts to date, many of which have been aimed at establishing norms for appropriate state behavior in cyberspace. These efforts include:

- The 1998 PDD-63 with guidance from Richard Clarke, former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism to commence working with like-minded and friendly states.

- Also in 1998 and following from PDD-63, an inter-agency strategy paper was penned, resulting in a four-track plan that was used for some 11 years. The strategy was aimed at engaging with other states on cybersecurity due diligence with like-minded states, i.e., all states would build up a capacity to defend their own networks under a four-pillar system organized nationally and aimed at modernizing substantial procedural law, building CERTs, fostering public-private partnerships, and building a public culture of awareness.

- In 2008, under the direction of Melissa Hathaway, the government undertook an exercise similar to Eisenhower's Solarium Project[25] aimed at promoting deterrence in cyberspace.[26] The project led to a broader strategy premised on building defenses as high as possible to keep out general malfeasance. Anything else would be treated as actions or threats emanating from traditional adversaries for which the government had sufficient experience in knowing how to deter and influence them. The strategy also demonstrated that there is no single bullet for deterrence; rather, what are needed are mutually overlapping international strategies that include promoting norms of appropriate state behavior in cyberspace supported by building confidence and security measures to ensure that states can operate with connectivity and collectively against disruptions and rogue states or non-state actors.

- The 2008 strategy was further developed in the 2011 International Strategy for Cyberspace. A principal objective of the strategy is to build a framework of principles of expected behavior supported by confidence- and security-building measures to which most nations, not all, will abide because it is in their ultimate security interest to do so.

Promoting norms and confidence-building measures at the international level

With the help of allies, as well as Russia and China, key steps have been taken on this difficult road, particularly within the UN Group of Governmental Experts (GGE), the first of which was established in 2005 pursuant to a Resolution tabled by the Russian Federation in 1998. Despite a difficult trajectory, in 2013, a third GGE finally reached agreement on the applicability of international law, particularly the UN Charter and Law of Armed Conflict (LOAC), to cyberspace, as well as the principles of sovereignty and state responsibility. The group also agreed that proxies used by states should be banned and it affirmed human rights. This was a significant achievement.

The United States has also focused on promoting and supporting transparency and confidence-building measures. In terms of transparency measures, the initial challenges of guaranteeing some form of predictability regarding cyberspace (key to transparency) was later overcome by the publication of U.S. 2011 *International Strategy for Cyberspace* and the 2011 Department of Defense *Strategy for Operating in Cyberspace* (DSOC) (unclassified version). Emphasis has also been placed on promoting the outcome of the UN GGEs in regional fora such as the OSCE, which, in December 2013, agreed on an initial set of confidence-building measures (CBMs) (11 in total).[27] While most of the CBMs relate to transparency measures, CBM 3 mandates mediated discussions between an aggressor and a victim (within the OSCE area of responsibility). At the NATO Wales summit earlier this year, all NATO members (28 of which are also OSCE members) affirmed that international law applies to state-on-state activity. CBMs have also been discussed within the ASEAN Regional Forum.

Finally, the current U.S. submission to the 2014 UNGGE provides a detailed examination of exactly how the UN Charter and the LOAC apply to cyberspace, including countermeasures and state uses of proxies. It also includes a vision of state sovereignty from the U.S. perspective. In addition, it advances *three new norms* of state behavior that the United States believes should apply to that spectrum of activity below the threshold of the use of force and for which there is no existing international legal precedent or source, but many.[28] Moreover, despite

what was discussed in Panel 2, the government is promoting these norms as a means to advance the fact that most cyber tools are used by non-state and state actors across a spectrum of conflict—most notably below the threshold of armed conflict.

Regardless of how they are defined (norms or confidence- and security-building activities or measures of self-restraint), it is evident that we are moving up a pyramid from transparency measures to cooperative measures and from there to measures of self-restraint, with these last measures the ones that will provide stability in the international environment. At the same time, it is important to bear in mind that CBMs and norms can only go so far. Russia's violations of norms applicable to the *kinetic* world in the Ukraine is a case in point.

Where to next then? The speaker suggested establishing an initiative similar to the Proliferation Security Initiative (PSI), a voluntary organization of like-minded states focused on interdicting the spread of fissile material. The idea would be to establish a similar voluntary organization made up of like-minded states that observe appropriate international norms, cooperate seamlessly against common cyber threats, refrain from destabilizing activity, and also come together in the future to sanction bad actors and to aid each other in mitigation and remediation. Establishing such an initiative is unlikely to happen any time soon, but that is the current vision.

3.3. Views from the Private Sector

From the perspective of the private sector representative on the panel, focus was placed on the need to work toward more *comprehensive planning* for *in*security, i.e., to help determine the most effective kind of contingency planning for dealing with the environment we are working in, to manage risk, now and in the future. Cyberspace challenges the traditional policy construct, not least because it changes so rapidly. And these changes are happening within a globally interconnected society, making it even more difficult to manage change. Some of the current issues regarding Internet governance might break that interconnectivity (at the domestic level), but the global connected nature of society will not change.

Participants discussed how, within that global interconnected society, government actors and a range of non-state actors, including the private sector, are involved in counter-risk operations, many of which have resulted in successful joint public-private operations.[29]

Conversely, today, the number of actors operating in cyberspace means that the potential for unintended consequences is significant.

In this sense, norms are actually being set by actions, rather than just through the kinds of state-centric deliberations discussed earlier. This is problematic. Certainly, considerable progress is being made, as noted with regard to the work of the Group of Governmental Experts, the OSCE work on CBMs, etc. Yet, that progress is being made at the high-end space of the United Nations. In reality; however, and as discussed by Panel 2 and above (regarding the U.S. submission to the 2014 GGE), the vast majority of the activity we are seeing now is below the threshold of armed conflict. Some of that activity can be addressed through standard response processes, but some requires more advanced response because of the urgency and severity of the risk to users. The vast majority of attacks requiring advanced response today are nation-state-sponsored.

Setting Norms for Below-the-Threshold Conflict

In an environment involving many different actors, tensions, and objectives operating below the threshold, it will be important to prioritize and think about an appropriate framework to guide both policymakers and the technical community. Such a framework can be centered on four components: understanding who the actors are (principally governments), the objectives, actions, and impacts as well as the global acceptance of the latter.[30]

For example, one of the difficulties in understanding impacts in cyberspace is that there is a tendency to group everything together (impact to users, national security, etc.). A more effective approach might be to break down the impact component even further. For example, when applying the concepts of distinction, discrimination, and reuse and managing the reuse of weapons (capabilities), those concepts don't actually look equal across the different technology environments.[31] Hence, it is important to be clear whether we are talking about commercial off-the-shelf technology, government off-the-shelf technology, operational technology, public cloud, private cloud, etc. And, when thinking about impacts and how to define norms that limit harm, it is also important to think about the information security attributes of the asset that may be affected, i.e., what is going to happen if the confidentiality, integrity, or availability of data is undermined. This focus is premised on the importance of trust—once trust in the data is lost (and it is unclear when it was lost) it is very difficult to regain.

The Private Sector: A Role in Norm-setting?

The panel discussed the importance of increasing participation of the private sector in different discussions on norms. Who is involved obviously depends on the issue, but in the context of international

security and stability, a significant number of ICT providers focused on infrastructure (ISPs, those building servers and databases), financial services organizations, oil and natural gas—all are operating on a multinational basis and all are key to ensuring stability. From an ICT provider perspective, certain things can be done, for example, working to reduce the attack surplus through secure engineering and working to manage supply-chain risk; coordinate and responsively disclose vulnerabilities within industry, i.e., reporting vulnerability to the vendor; cooperating to address open-source vulnerabilities; share information that helps limit the scope and impact of incidents that do occur; and participate in response and recovery activities.

Pending Policy Issues

A core dilemma relates to U.S. capacity to influence outcomes at a time when the reputation of the U.S. government and U.S. ICT providers in their uses of cyberspace and ICTs is at an all-time low. This is occurring at a time of complex geopolitical shifts in which normative disintegration and disengagement are affecting many areas and many contexts, not just cyberspace and cybersecurity.

- Does this place the United States at a strategic disadvantage in terms of being able to influence normative outcomes with regard to cyberspace?

- Will pragmatism be the way forward? Pragmatism, it was suggested, does not imply the cancellation of vision, objectives, or goals, but rather shifts focus to the definition of the acceptable futures we can live with. It can allow us to think along the lines of converging interests—i.e., where things are coming together (for example, the converging interests of the United States and China in the area of financial stability). Is this a viable way forward? Is it consonant with current strategy and foreign policy?

- Within this shifting geopolitical context, what are the opportunities and challenges of establishing a PSI-like initiative to support the propagation and implementation of norms for state behavior in cyberspace as suggested during the panel discussion?

NCAFP POLICY RECOMMENDATIONS

As evidenced in this report, a range of outstanding issues relating to cybersecurity still need to be addressed and resolved. At the higher level, core questions raised throughout the meeting related to whether the current U.S. strategy is producing results and how the

United States envisages influencing outcomes in a shifting and complex global geopolitical environment in which normative disengagement is increasing and in which the United States itself has undermined some of the normative values it is hoping to promote and project into cyberspace and the Internet. The latter relates to the increasing tensions and trade-offs between national security prerogatives on the one hand and privacy or broader human rights on the other. The recrudescence of terrorism, particularly in the form of the Islamic State and its use of the Internet for recruitment and propaganda purposes, has not helped. Nor, indeed, has the growing state uses of ICTs for malicious purposes. Furthermore, the focus of several states on asserting or pushing for controls over the Internet (and for many, the information flowing through it) presents a number of important policy dilemmas for the United States that need to be reconciled.

Undoubtedly, significant progress is being made to respond to growing cybersecurity challenges. Over the next 12–18 months, the United States will participate in a number of processes relating to international and regional security, governance, human rights, counter-terrorism, trade, and development—all of which are directly or indirectly related to cyberspace, the Internet, and the uses of ICTs by state and non-state actors. Moving forward, policy experts might consider the outstanding issues and policy dilemmas outlined in this report and summarized here:

- How does the U.S. policy community consider the projection of U.S. cyber power in the context of the global geopolitical and strategic changes currently under way (multi-polarity and the gradual diffusion of power away from the West, the increasing assertiveness of middle-income states in different regions; a recrudescence of extremism and organized crime across regions, the increasing use of special operations forces, etc.)? Does the current U.S. International Strategy for Cyberspace respond to these realities? How tight are the linkages between this strategy and other areas of foreign policy? Is it time to review progress relating to the implementation of the Strategy? How might such a review be conducted?

- A major focus of the 2011 U.S. International Strategy on Cyberspace is aimed at influencing normative outcomes with regard to cyberspace. How can the United States more effectively respond to the extension of sovereignty into cyberspace and over ICTs in general by states that do not share the same values or goals as the United States and its partners? How can the United States

and its allies continue to influence or shape other states' behavior in this regard if they themselves are struggling with questions of waning normative legitimacy?

- Within this shifting geopolitical context, what are the opportunities and challenges of establishing a PSI-like initiative to support the propagation and implementation of norms for state behavior in cyberspace as suggested during the panel discussion?

- Will current norm-setting processes continue to be strictly state-led and aimed at establishing a comprehensive regime for cyberspace or will the special characteristics of cyberspace lead to a shift in focus, with attention centered more on specific issue areas such as terrorism, crime, or supply-chain integrity?

- A number of efforts aimed at setting norms for "below-the-threshold" malicious activity in cyberspace are emerging. Are they sufficient? How can other states and stakeholders be engaged in this area?

- Will the United States push for greater engagement with non-state actors such as the private sector, certain civil society organizations, and academia in these norm-setting processes at domestic, regional, and international levels? If so, what would such engagement involve?

- To what extent should discussions on the use of cyber capabilities be linked to ongoing discussions on the weaponization of automized technologies/robotics?

- What are the national security implications of our increasing reliance on special forces (including specialized units with enhanced cyber and autonomous capabilities) for tactical purposes (i.e., as employable capability) in foreign theaters where we are not at war in the traditional sense? What challenges or opportunities does the deployment of special forces represent for the exercise of other instruments of national power and ensuring stability in the international system?

1. According to the moderator, for many of the G20 countries, integrating access to the Internet holds a promise of at least 4% of GDP growth. For developing economies that promise can be as high as 10%.
2. Melissa E. Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," *American Foreign Policy Interests* 36, no. 5 (2014): 300–313.
3. For example, India has three landing stations. If they are damaged, India would be off the grid for

at least six weeks. And India would not be the only country affected. A growing number of U.S. corporations run their back offices from India and would thus be equally affected.

4. For further insights into issues pertaining to data sovereignty, see, Tim Maurer et al. *Technological Sovereignty: Missing the Point? An Analysis of European Proposals After June 5, 2013*. Transatlantic Dialogues on Security and Freedom in the Digital Age, http://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf
5. According to the moderator, some 107 states field special operation forces that lean on cyber and IW capabilities for a range of missions, including strategic reconnaissance, intelligence, unconventional warfare, and direct action/special warfare.
6. See, in particular, William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Random House, 1996).
7. Regarding how cyberspace is key to operational security, the operation to bring down Osama bin Laden is an interesting example. Preparations for the operation had covered every aspect of the electromagnetic spectrum as part of the operational security plan; yet they had overlooked Twitter. As the helicopters were hovering over bin Laden's residence in Abbotabbad, Pakistan, a Voice of America stringer, who happened to be in the area of operations tweeted nine times the presence of U.S. troops in the area.
8. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a forum for states to agree on which specific technologies should be subject to export control for regional and international security and stability purposes. See: http://www.wassenaar.org
9. See Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance Updating Export Controls to the Digital Age," 2014, New America Foundation, http://oti.newamerica.net/publications/policy/uncontrolled_global_surveillance_updating_export_controls_to_the_digital_age
10. See Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Spring 2011.
11. For a deeper discussion on these points of scale, proximity, and precision, see Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (Spring 2014).
12. See, for example, "Framing Questions on the Weaponization of Increasingly Autonomous Technologies," UNIDIR, 2014, http://www.unidir.org/files/publications/pdfs/framing-discussions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf
13. Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 34, no. 5 (2014): 322–331.
14. See Duncan Hollis, "Neither Cacophony Nor Concert: Minor Notes on Metanorms for Cyberspace." https://prezi.com/l2rzahogaatm/neither-cacophony-nor-concert-minor-notes-on-metanorms-for-cyberspace/?utm_source=prezi-view&utm_medium=ending-bar&utm_content=Title-link&utm_campaign=ending-bar-tryout
15. See Peter Katzentein, ed. *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996).
16. National Institute of Standard and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" of February 2014. This was developed following President Obama' Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, of February 2013.
17. Hollis.
18. Michael N. Schimtt, ed., *Tallinn Manual on the International Law Applicable to Cyberspace* (Cambridge: Cambridge University Press, 2013).
19. UN General Assembly Resolution "The Right to Privacy in the Digital Age," A/RES/68/1670 of 21 January 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/ r68_en.shtml&Lang=E
20. See European Commission, "Factsheet on the 'Right to Be Forgotten' Ruling," http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
21. See Global Commission on Internet Governance, https://www.ourinternet.org/#about
22. ICANN, "Montevideo Statement on the Future of Internet Cooperation," https://www.icann.org/news/announcement-2013-10-07-en
23. For an insight into the stewards vs. sovereigntist debate, see the Munk School of Global Affairs 2012 Cyber Dialogue, http://www.cyberdialogue.ca/previous-dialogues/2012-about/papers/
24. See Cass R. Sunstein, "Incompletely Theorized Agreements," *Harvard Law Review* 108, no. 7 (May

1995): 1733–1772. The panelist noted in particular Sunstein's emphasis on the norm of religious liberty. Some people favor it because of their own religious beliefs; others for utilitarian reasons; security officials because it preserves the social peace, etc. We don't have to agree on why religious liberty is a norm; we just accept it and move on.

25. See William B. Pickett, ed., *George F. Kennan and the Origins of Eisenhower's New Look: An Oral History of Project Solarium*, Princeton Institute for International and Regional Studies, Monograph Series, No. 1 (Princeton, N.J.: Princeton University, 2004).
26. For a discussion on the outcome of the exercise, see, John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 25, 2010.
27. For an overview of the OSCE CBMs and other related processes, see Camino Kavanagh et al. "Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security," ICT for Peace Foundation, http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/
28. The three new norms advanced by the U.S. government include:
    1. States should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure that provides services to the public.
    2. States should not conduct or knowingly support activity intended to prevent national C-CERT from responding to cyber incidents and a state should not use C-CERTs to enable online activity that is intended to do harm.
    3. States should cooperate in a manner consistent with international law and its international obligations with requests for assistance from states in investigating cyber crimes and collecting electronic evidence and mitigating malicious cyber activity emanating from its territory. States must take immediate and robust action to investigate criminal activity by non-state actors.
29. For example, in response to the 2012 DDOS attacks against U.S. banks, the government and private sector worked together using both tech and diplomatic channels to address and stem the threat. In 2013 and 2014, we have witnessed several successful international and domestic Botnet takedowns with massive implications for users.
30. Building on an initial framework presented at the 2013 RSA, Microsoft presented a paper at the EWI Cyber Summit in Berlin in December 2014, proposing six specific norms aimed at limiting conflict in this space. See "International Security Norms: Reducing Conflict in an Inter-dependent World," Microsoft, December 2014.
31 For example, when a vulnerability is exploited in commercial off-the-shelf technology for national security purposes, the possibility of reuse of that vulnerability is very high. When looked at from the perspective of government off-the-shelf technology, it will be more narrow. If a public cloud is attacked, the consequences will probably be very high; a private cloud, less so.

National Committee on American Foreign Policy, Inc.

FOUNDER – Dr. Hans J. Morgenthau

MORGENTHAU AWARD RECIPIENTS

Honorable Angier Biddle Duke
Honorable Sol Linowitz
Honorable Henry A. Kissinger
Honorable Jeane J. Kirkpatrick
Honorable George P. Shultz
David Rockefeller
Honorable James A. Baker III
Right Honorable Margaret Thatcher
Honorable Thomas R. Pickering
His Majesty King Hussein
Honorable Colin L. Powell
Honorable Richard N. Haass
Honorable Martti Ahtisaari

KENNAN AWARD RECIPIENTS

Honorable George F. Kennan
Honorable Cyrus R. Vance
Honorable Paul A. Volcker
Honorable Richard C. Holbrooke
Maurice R. Greenberg
Honorable John D. Negroponte
General David H. Petraeus
Commissioner Raymond W. Kelly
Honorable Karl W. Eikenberry

THE WILLIAM J. FLYNN INITIATIVE FOR PEACE AWARD RECIPIENTS

William J. Flynn
Honorable George J. Mitchell
Right Honorable Dr. Marjorie Mowlam
Viola Drath
Honorable Hugh L. Carey
Gerry Adams, M.P.

GLOBAL BUSINESS LEADERSHIP AWARD RECIPIENTS

Dr. Paul E. Jacobs
Mr. Muhtar Kent
Mr. William R. Johnson

HUMANITARIAN AND PEACE AWARD RECIPIENT

Professor Elie Wiesel

21ST CENTURY LEADER AWARD RECIPIENTS

Dr. Nancy Walbridge Collins
Dr. John P. Delury
Abraham M. Denmark
Ronan Farrow
Nathaniel C. Fick
Brendan R. McGuire, Esq.
Marisa L. Porges
Farhana Qazi
Joshua Cooper Ramo
Nicholas Thompson

OFFICERS 2013-2014

Honorable Paul A. Volcker–*Honorary Chairman*
William J. Flynn–*Chairman*
Dr. George D. Schwab–*President*
William M. Rudolf–*Executive Vice President and Treasurer*
Donald S. Rice, Esq.–*Senior Vice President*
Professor Donald S. Zagoria–*Senior Vice President*
Edythe M. Holbrook–*Vice President*
Hatice U. Morrissey–*Vice President*
Grace Kennan Warnecke–*Vice President*
John V. Connorton, Jr., Esq.–*Secretary*

TRUSTEES

*Kenneth J. Bialkin, Esq.
*Honorable Donald M. Blinken
Steven Chernys
*Professor Michael Curtis
Mary Wadsworth Darby
Honorable Karl W. Eikenberry
Judith Hernstadt
Thomas J. Moran
*Honorable Matthew Nimetz
Honorable Thomas R. Pickering
Honorable Jeffrey R. Shafer
Honorable Nancy E. Soderberg

* Executive Committee

BOARD OF ADVISERS

Dr. Giuseppe Ammendola
Professor Kenneth J. Arrow
Professor Stephen Blank
Professor Bernard E. Brown
Professor Ralph Buultjens
Honorable Herman Cohen
Dr. Alexander A. Cooley
Dr. Eve Epstein
Professor Joseph W. Foxell
Dr. Susan A. Gitelson
Professor George E. Gruen
Professor Bernard Haykel
Honorable Robert E. Hunter
Dr. Ephraim Isaac
Dr. Jeffrey Mankoff
Dr. Jeffrey D. McCausland
Aaron David Miller
Joan Peters
David L. Phillips
Professor Richard Pipes
Dr. Carol Rittner
Professor Benjamin Rivlin
Professor Henry Rosovsky
Professor Michael Rywkin
Marcus H. Sachs
Dr. Ronald J. Sheppard

NATIONAL COMMITTEE ON
AMERICAN FOREIGN POLICY, INC.
320 Park Avenue
New York, N.Y. 10022
Telephone: (212) 224 1120 • Fax: (212) 224 2524
E-Mail: contact@ncafp.org • Web site: http://www.ncafp.org