STATEMENT FOR THE RECORD

by

SEAN KANUCK

for

United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Information Technology
Subcommittee on National Security

Hearing entitled

"Digital Acts of War: Evolving the Cybersecurity Conversation"

13 July 2016

2:00 pm

Rayburn House Office Building

Room 2154

Chairman Hurd, Chairman DeSantis, Ranking Member Kelly, Ranking Member Lynch, and distinguished Members of Congress:

It is my honor and privilege to participate in the hearing entitled "Digital Acts of War: Evolving the Cybersecurity Conversation" before the Subcommittees on Information Technology and National Security of the Committee on Oversight and Government Reform of the House of Representatives. I thank you for your invitation and sincerely hope that my contribution will assist you in your work on this critical topic.

This Statement for the Record draws upon my twenty years of experience in the field of information and communication technologies (ICT), including: as an academic, as a professional attorney who specializes in public international law, and as a senior intelligence officer for the United States Government. The perspective offered herein has been ineluctably shaped by my service as the National Intelligence Officer for Cyber Issues (NIO/Cyber) from May 2011 to May 2016. Having led strategic cyber analysis for the US Intelligence Community for five years, I earnestly concur in the need to evolve the cyber security conversation beyond where it is today. That will require (1) deeper subject matter expertise by more policy makers and legislators, (2) broader inclusion of private sector concerns and recommendations in public policy, and (3) a genuinely strategic approach that is currently lacking.

Since 2013, the Director of National Intelligence has led his annual, written Worldwide Threat Assessment to Congress with the cyber topic because ICT not only pose a cyber security risk in their own right, but also are integral factors utilized in the conduct of nearly every national security threat today.[1] During my tenure as NIO/Cyber, the US Intelligence Community attempted to provide policy makers with a strategic framework to understand cyber threats and strove to dispel several misnomers about cyberspace, namely: (a) it is not a unique physical "domain"; (b) it does not fulfill the logical criteria of a "global commons"; (c) not all adversarial cyber operations qualify as "attacks"; and (d) a "cyber Armageddon" is a highly improbable scenario. Rather than revisiting those questions that have been previously addressed elsewhere, this Statement will simply take those understandings as its point of departure.[2]

In order to evolve the cyber security conversation, one must first know what has or has not already been established and/or achieved. For example, the question of what constitutes a digital act of war has been studied for over twenty years. Rigorous legal scholarship by both myself and Michael Schmitt in the mid-to-late 1990s concluded that an effects-based analysis would be required to assess the applicability of Articles 2(4) and 51 of the United Nations Charter.[3] Most academic commentators around the world who subsequently turned to that same question have arrived at a similar conclusion. The extreme difficulty of observing or detecting actions in cyberspace – let alone divining intentions – leaves one with effects as the only legitimate measure upon which to base policy responses. The academic, non-binding Tallinn Manual (for which Michael Schmitt has served as editor) perhaps now offers the strongest and most articulate exegesis of the effects-based doctrine.[4] It essentially says that what constitutes an act of war is

largely agnostic of the modality used to perpetrate the harm(s). Accordingly, a special notion of a "digital" act of war is yet another misnomer.

Politicians and the media may try to label significant espionage successes or compromises of personally identifiable information (PII) as acts of cyber war, but such parlance does not comport with legal reasoning. That does not mean that a wide array of policy options – ranging from demarches to sanctions to domestic law enforcement or counterintelligence measures – can not be leveraged to dissuade such activities. Rather, it highlights the complexities of the strategic ICT environment whereby sovereign powers are particularly susceptible to foreign intervention in their internal affairs. In fact, fixation on defining the precise threshold for a digital act of war (beyond the de facto effects-based analysis to be applied in any actual scenario) distracts from the important question of how cyber operations are actually being used today. They tend to occur in one of four types: (i) operational preparation of the environment for use during future kinetic military conflict (wherein the question of a digital act of war trigger would be much less relevant); (ii) espionage (which is not addressed by public international law); (iii) criminal activity by non-state actors (which is not the usual basis for declarations of war or military reprisals); and (iv) willful intervention below the threshold of armed conflict.

My experience as an intelligence analyst has led me to believe that most adversaries use cyber operations as a strategic alternative to armed conflict and intend to conduct such activities with the deliberate objective of avoiding military retaliation by their targets. The famous strategist Sun Tzu would applaud the use of such means to accomplish one's goals without engaging in costly combat. To concentrate predominantly on the issue of what constitutes an act of war in cyberspace largely misses the strategic appeal of asymmetric cyber capabilities. The entire purpose of many cyber operations is to exert coercive influence without engendering an international armed conflict.

A more worthy focus might be considering what progress has been achieved to date in establishing rules, norms of behavior, or confidence building measures for actions in cyberspace. 2015-16 was a benchmark year for non-binding diplomatic expressions of proposed rules of behavior (i.e. norms) for state actors in cyberspace. In July 2015, a United Nations Group of Governmental Exports (GGE) report was issued that not only reaffirmed the applicability of international law and the United Nations Charter to activities in cyberspace, but also recommended several normative principles – most notably for limiting cyber attacks against civilian critical infrastructures.[5] In September 2015, Presidents Obama and Xi reached an accord to proscribe state-sponsored cyber espionage for commercial gain, which was later embraced by the Group of 20 (G-20) leaders in their joint statement from November 2015.[6] Finally, in March 2016, the Organization for Security and Co-operation in Europe (OSCE) issued its decision on confidence building measures to reduce the risk of ICT conflicts.[7]

While those expressions can be politically expedient and may contribute to the formation of customary international law over lengthy periods of time, one must nonetheless query what – if anything – has changed in the actual behaviors of cyber actors since those diplomatic pronouncements. I would offer that some nations may have altered their modus operandi or

adjusted their target sets to some degree, but that the overall security of cyberspace has not been appreciably strengthened. In fact, one can make a reasoned argument that cyberspace is an increasingly contested, vulnerable, and volatile environment despite those diplomatic overtures. To my knowledge, no nation – not even the United States or our closest allies – has declared a sincere interest in outlawing the use of any particular cyber capability under all circumstances. Instead, prohibitive discussions have mainly centered on types of targets that are to be avoided where possible, which although consistent with the effects-based approach mentioned above does little in the way of creating tangible incentives for compliance with such rules. For example, despite the normative proposals cited above, private sector utilities (e.g. in the energy sector) and other critical ICT infrastructures remain preferred targets for cyber operators.

International negotiations regarding ICT are unlikely to yield concrete, enforceable rules of behavior in the near term because different nations have fundamentally different political objectives for those discussions. The United States defines cyber security primarily in the context of critical infrastructure protection (i.e. keeping the "pipes" up and running), while nations like Russia and China are equally concerned about regulating the informational content transiting those networks.[8] A failure to appreciate the import of that strategic distinction might lead one to overestimate the potential impact of diplomatic efforts on actual behaviors (overt, clandestine, or covert). In April 2016, the Russian Federation's lead cyber negotiator even expressed that the range of possible compromise achievable within the GGE framework might have been "exhausted" already.[9]

Since no country seems genuinely eager to forego its sovereign prerogative to develop offensive ICT capabilities and/or conduct cyber operations for national advantage, the international community is left with a Hobbesian paradigm wherein the infamous adage from the Melian Dialogue rings true, namely: "The strong do what they can, and the weak suffer what they must." Given that unsettling reality, further inquiry into the causes of that systemic result is warranted.

The burden of proof currently lies with the victim to establish definitive attribution for an adverse cyber incident. Attribution has two essential components, and any policy decision to publicly attribute an incident (if positive attribution can be established) must be based on three additional considerations. As NIO/Cyber, I advocated a dualistic approach that included both technical attribution (i.e. forensic investigation of the victim's ICT networks, reverse engineering of malicious software code, etc.) and analytic attribution (i.e. an all-source intelligence assessment of potential perpetrators, their possible motivations, the geo-political context, and other expected indicators that might support each hypothesis). Detailed analysis and comparison of historic cyber events illustrate that different types of actors conduct different kinds of operations against different kinds of targets. Each has its own motivations and concerns which necessarily influence what kind of effects it perpetrates and/or what it does with any stolen data. For example, one would expect the "take" from a state sponsored theft of PII from a healthcare of financial institution to be handled much differently than if the same target had been compromised by a criminal element seeking to maximize the monetary value of that information. A holistic attribution assessment must take all of these factors (technical and contextual) into consideration.

Despite significant advances by both public and private sector cyber security researchers in recent years, it still remains difficult to reach high-confidence attribution assessments within the "real time" parameters that would be required for executive decision making during an incident.[10] That necessarily leaves one in a post hoc reactive mode, and even if one eventually reaches an attribution determination, then the next grouping of considerations comes into play.

Any decision regarding whether or not to publicly attribute a cyber event must account for (1) the bilateral and/or multilateral political ramifications of making such an accusation, (2) the relative costs and benefits of disclosing the evidence required to substantiate an attribution statement, and (3) whether or not one is willing and/or able to punish the perpetrator to whom the event is to be attributed. In this regard, the political decision about the merits of public attribution is wholly independent from the underlying factual question about attribution. One can easily imagine scenarios where one nation may not choose to publicly confront an ally, a trading partner, or a key creditor nation. But, the dilemmas posed by the second and third considerations are even more difficult.

Cyberspace is possibly unique in that the victims of adverse events have a very strong incentive not to publicly prove what has been done to them and by whom. That is owing to the fact that the very same kinds of ICT, methodologies, and accesses that are used for cyber intelligence operations are also used for cyber attack operations. Accordingly, a revelation of evidence that could compromise sources and methods for future intelligence collection might also enable an adversary to develop countermeasures for national military capabilities as well. In other contexts, such as the nuclear model, the technological platforms for intelligence and reconnaissance are distinct from the platforms required for a retaliatory strike. Strategically speaking, no such bifurcation of platforms exists in the cyber arena – which in turn provides a strong disincentive, or at least a very high threshold, for any nation's willingness to "prove" an attribution assessment for the international community writ large.

Another strategic consideration for public attribution relates to global power dynamics. If a nation has declared certain offenses to be unacceptable and announces that one has occurred, its reputation and the credibility of its deterrent mechanisms are then put to the test. Therefore, one can infer that nations might not wish to publicly attribute events for which they know they cannot exact satisfaction. And that dilemma is only exacerbated by the fact, mentioned above, that cyber capabilities are perishable once revealed. There is no analogue to a standing navy in port or intercontinental ballistic missile silo whose mere existence serves as a credible deterrent. In essence, today's cyber strategist would not be inclined to disclose specific offensive cyber capabilities unless she was prepared to use them imminently. Once again, the clear disincentives to publicize retaliatory capabilities or declaratory redlines – and even to prove that one was victimized – all render the cyber dialogue uncharacteristic of other strategic policy discussions.

High-confidence, public attribution remains one of the most pertinent topics in international cyber conferences. On the one hand, it seems like a natural prerequisite for any legitimate accusation or reprisal. But, on the other hand, the technical realities of cyberspace

currently permit offenders to either evade punishment (based on insufficient public attribution) or else inflict further policy dilemmas and security compromises on the already afflicted victim.

The market for cyber intelligence has grown propitiously. Governments around the world now benefit from thousands of cyber security analysts in the private sector who are monitoring networks, remediating incidents, and investigating breaches around the clock. Private companies are also increasingly providing threat intelligence that is steadily approaching the all-source format used by governmental intelligence agencies and security services. Personally, I welcome that expanded industry focus from a defender's perspective even though I must also acknowledge that it complicates certain US military, intelligence, counterintelligence, and law enforcement missions.

The private sector already owns and operates much of the critical infrastructure in the United States. It is also increasingly positioned to provide cyber threat intelligence and high quality attribution assessments. And private companies are also increasingly being targeted by a broad range of illicit cyber actors, whether as part of geo-political conflicts or by profit-motivated criminals. Any public policy discussions regarding cyber deterrence, norms of behavior, or strategic implications for US national and economic security that do not take account of private sector input should be considered lacking. That is not to say that the US Government should defer to corporations on sovereign matters, but rather that it must acknowledge that it no longer leads technological innovation for the nation or suffers the primary brunt of conflicts in cyberspace.

Another interesting observation from my analytic outreach to many industry professionals and academic international relations theorists over the years has been the centrality of improved resiliency for maintaining the fullest breadth of one's own national security policy options. As the preceding discussion about attribution and credible deterrents alluded, the weaker one's own cyber capabilities are, the more limited one's policy options will be in the face of an adversary's transgression. So it is very noteworthy, albeit counterintuitive, that a strong cyber offense requires an equally strong if not stronger cyber defense. That is what permits the freedom of maneuver.

In the case of the United States, that represents a call for improved cyber security practices across public utilities and other critical infrastructures throughout multiple sectors. It remains unclear if legislation, regulation, or market forces will eventually induce the desired result. It also remains unclear how US-based multinational corporations will navigate an increasingly complex environment of data privacy, data retention, encryption, event disclosure, and surveillance laws from multiple jurisdictions (both domestic and foreign). In the interim, I envision that the nascent cyber insurance market, along with heightened reporting requirements for data breaches or other cyber events by the Securities and Exchange Commission, will begin to incentivize companies towards adopting best practices for cyber security. That will in turn bolster other governmental efforts, such as the Cybersecurity Framework promulgated by the National Institute of Standards and Technology (NIST) at the Department of Commerce.

I cannot purport to have solutions for all of the policy challenges that I have outlined in this Statement; however, with the Subcommittees' indulgence, I will offer some limited recommendations for consideration going forward:

- Concerted thought is required on the strategic realities that would be both necessary and sufficient to create an effective deterrent to foreign and domestic cyber threats. One cannot presume that diplomatic overtures automatically translate into behavioral changes, or that international law will not be honored in the breach.

- New normative frameworks should be considered which accept the prevalence of cyber operations – including against private sector targets during peacetime – and instead focus on holding actors strictly liable for any and all effects (intended or otherwise) caused by their deliberate actions.[11] Some form of enforcement mechanism is required to better constrain offensive cyber activity.

- US policy makers should consider the potential benefits of clear, declaratory redlines in cyberspace as well as the use of overt cyber operations where it is determined that US military or law enforcement action is warranted. The strategic uncertainty in cyberspace is partly owing to the ubiquitous use of clandestine operations to evade attribution and obfuscate sovereign influences.

- Improved cyber defenses and resiliency are required throughout US critical infrastructures in order to provide US policy makers the greatest breadth of policy options when confronted with adversarial events. Perfect cyber security is impossible, so risk mitigation and risk management models must be employed to maintain core operations and enterprise value even in a degraded environment.

- The US private sector should be consulted more thoroughly in connection with national policy decisions whose impact will be borne by those companies. Military and diplomatic strategies that could indirectly harm the US economy by imposing additional transaction costs, inducing foreign retaliation against US companies, or concealing dangerous vulnerabilities that can be exploited by our adversaries should receive careful review.

- Public agencies in the United States face extreme challenges in recruiting and retaining world class ICT talent. Cyber expertise is a qualitative vice quantitative endeavor (i.e. the number of congressionally authorized billets matters less than who is filling those billets). Additional consideration should be given to ensuring that the US Government employs more of the cyber "Olympians".

Once again, thank you for this opportunity to provide service to my country.

Respectfully submitted by Sean Kanuck.

[1] See: James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 12 March 2013; James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 29 January 2014; James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, 26 February 2015; and James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, 9 February 2016.

[2] For discussion regarding points (a) and (b), see Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law" in Texas Law Review, Volume 88, Number 7, June 2010 (pages 1573-1580). For discussion regarding point (c), see James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, 12 March 2013 (page 1). For discussion regarding point (d), see James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, 26 February 2015 (page 1).

[3] See Sean P. Kanuck, "Information Warfare: New Challenges for Public International Law" in Harvard International Law Journal, Volume 37, Number 1, Winter 1996 (page 292). See generally, Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" in Columbia Journal of Transnational Law, Volume 37, 1999.

[4] See generally, Tallinn Manual on the International Law Applicable to Cyber Warfare, North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence, 15 March 2013.

[5] See "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly document A/70/174, 22 July 2015. See also, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly document A/68/98, 24 June 2013.

[6] See the White House press release entitled "Fact Sheet: President Xi Jinping's State Visit to the United States" dated 25 September 2015, and the "G20 Leaders' Communiqué" from the Antalya Summit held on 15-16 November 2015.

[7] See Decision Number 1202 of the Permanent Council of the Organization for Security and Co-operation in Europe entitled "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies" dated 10 March 2016. See also Decision Number 1106 of the Permanent Council of the Organization for Security and Co-operation in Europe entitled "Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies" dated 3 December 2013.

[8] See generally: White House press release regarding Presidential Policy Directive/PPD-21 entitled "Critical Infrastructure Security and Resilience" dated 12 February 2013; Executive Order 13636 of 12 February 2013 entitled "Improving Critical Infrastructure Cybersecurity" in Federal Register, Volume 78, Number 33, 19 February 2013; United Nations General Assembly document A/69/723, Annex entitled "International code of conduct for information security", 13 January 2015; and Shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 16 June 2009.

[9] Statement made by Andrey Krutskikh to US Government officials on the margins of the United Nations Institute for Disarmament (UNIDIR) workshop entitled "The Application of International Law in the Context of International Cybersecurity" held in Geneva, Switzerland from 19-21 April 2016.

[10] See generally, James R. Clapper, Director of National Intelligence, Statements for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, 9 February 2016 (page 3) and 26 February 2015 (page 2).

[11] See e.g., proposed norm number 22 in The Hague Centre for Strategic Studies working paper for the Global Conference on Cyber Security entitled "Food for thought for break-out group 'Confidence Building Measures, Norms of Behavior and Public-Private Cooperation for International Security in Cyberspace'" presented on 17 April 2015 in The Hague, Netherlands.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: SEAN KANUCK

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

NO GRANTS OR CONTRACTS.
I WAS EMPLOYED AS A CIVIL SERVANT BY THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI) FROM MAY 2011 TO MAY 2016.

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

I AM TESTIFYING IN MY PERSONAL CAPACITY.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

NOT APPLICABLE.

I certify that the above information is true and correct.
Signature: Sean Kanuck Date: 11 JULY 2016

SEAN KANUCK, ESQ.

Legal & Strategic Consulting Services

Executive Leadership for Global Challenges

Information Technology • National Security • Risk Analysis • Corporate Strategy • International Law

- *Visionary leader with proven success building national-level enterprises and managing complex programs*
- *Internationally recognized expert with 20+ years experience in cyber security and information operations*
- *Senior US Government official and diplomat who has worked directly with many international institutions*
- *Author and keynote speaker for global audiences on the nexus between law, technology, and security*

2011-2016 **NATIONAL INTELLIGENCE OFFICER FOR CYBER ISSUES, ODNI**

- 5-year senior executive appointment to lead cyber analysis for the US Intelligence Community
- Founder and director of a new strategic office within the National Intelligence Council
- Principal cyber threat adviser to the National Security Council and President's Daily Brief
- Conducted more than 50 intelligence briefings and testimonies for Congressional committees
- Accurately forecasted technology trends and established new information security models

2009-2010 **GROUP OF GOVERNMENTAL EXPERTS, UNITED NATIONS**

- Member of US delegation to the General Assembly's forum on international information security
- Participated in diplomatic negotiations with the BRICS countries to develop global cyber norms

2007-2009 **NATIONAL SECURITY COUNCIL, WHITE HOUSE**

- Intelligence Fellow with the Directorates for Combating Terrorism and Cyber Security
- Contributing author on law and strategy for the 2009 White House Cyberspace Policy Review

2000-2007 **INFORMATION OPERATIONS CENTER, CIA**

- Original member of the Directorate of Intelligence's all-source cyber threat analysis unit
- 3-year field assignment establishing cyber security cooperation with 10 European countries
- Designed and led innovative counter-terrorism programs with allied nations
- Inducted into the Senior Analytic Service and Exceptional Intelligence Officer Program

1997-2000 **ATTORNEY, SKADDEN ARPS**

- Associate in the Mergers & Acquisitions, Corporate Finance, and Banking departments
- Represented Fortune 100 clients for mergers, securities offerings, and credit facilities
- Counseled international project financing in the global telecommunications and energy sectors

1996-1997 **FREDERICK SHELDON TRAVELING FELLOW, HARVARD UNIVERSITY**

- Independent travel and study abroad in Western Europe, Russia, and Sub-Saharan Africa

UNIVERSITY OF OSLO, LL.M. in Public International Law	2008
LONDON SCHOOL OF ECONOMICS, M.SC. in International Relations	1997
HARVARD LAW SCHOOL, J.D. (cum laude)	1996
HARVARD COLLEGE, A.B. (magna cum laude) in Government & Philosophy	1993

- Admitted to the Bar in New York and the District of Columbia
- Trustee of the Center for Excellence in Education (based in Virginia, USA)
- Member of the International Institute for Strategic Studies (based in London, UK)
- Extensive foreign travel and business experience in over 50 countries on 6 continents