STATEMENT OF

CHRIS INGLIS

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

27 April 2017

VERSION: 23 April 2017

Thank you, Chairman Rounds, Ranking Member Nelson, and Members of the Committee. I am pleased to appear before you today to talk on the topic of cyber enabled information operations.

As the committee noted in its invitation, “information operations” have been conducted as a component of state and non-state operations for centuries but have recently taken on significantly greater import because of the leverage, speed, scope and scale afforded them by the technologies and trends attendant to the rise of the internet.

My comments today are derived from twenty-eight years of experience at the National Security Agency working both of its related but distinguished missions: the Information Assurance mission supporting the defense of critical information and networks, and the Signals Intelligence mission which generates foreign intelligence needed to inform the Nation’s defense. While I possess technical degrees in engineering and computer science, the majority of my career at the National Security Agency was spent in leadership positions, including seven and one half years’ service as NSA’s senior civilian and Deputy Director during the period 2006-2014. Since July 2014, I have also served on several Defense Science Board studies on the topic of cyber, and as a visiting professor of cyber studies at the United States Naval Academy, which has been developing and delivering cyber education for future Naval and Marine Corps officers for several years. While the views I will express are necessarily mine alone, I will draw from the sum of these experiences in these opening remarks and throughout the question and answer period.

The committee’s invitation letter asked for perspectives on the changes in **“scale, speed, and precision [afforded] by modern cyber hacking capabilities, social media and large-scale data analytics” as well as views on “technical, organizational, and operational means needed to detect and counter these operations, including public-private collaboration and international efforts.”**

I will address these in brief opening remarks and welcome the opportunity to discuss in greater detail during the hearing’s question and answer session.

The revolution afforded by the internet over the past forty years is one fueled by innovations in technology and the private sector's ability to deliver that innovation at scale and with supporting infrastructure to billions of consumers in an increasingly global marketplace.

While technology revolution is the visible phenomenon, there are several trends that greatly influence the impact of technology on society at large. I describe three such trends here that, while not independent of technology, are distinct from it, even as they exacerbate its effects.

- The first is a new geography wherein people and organizations increasingly see the internet as a jurisdiction in its own right, a jurisdiction that transcends the physical limitations and legal jurisdictions once defined by physical geography alone. The effects of this phenomenon necessarily attenuate the influence of governments and other jurisdictions that are based on physical borders. That fact notwithstanding, the impact can be quite positive, as in the case where the allocation of goods and services are optimized on a global basis, smoothing out sources, flows, and consumption; or quite negative, wherein the challenges of reconciling legal jurisdiction and the inherent difficulty of cyber attribution conspire to increase the challenge of achieving reasonable enforcement of legal norms in and through cyberspace.
- The second is a new social order wherein people increasingly organize by ideology as much or more by physical proximity alone. As with the new geography, the impact of this can be perceived as good or bad. The sweep of democratic ideals across many nations in the 2011 Arab Spring was largely borne of this phenomenon. In a similar manner, radicalization of lone wolf terrorists who are inspired to acts of terror without ever meeting their mentors makes use of the same mechanism. Wikileaks too is borne of this phenomenon – a force in the world that knows no physical borders even while it has an increasing effect – sometimes favorable, sometimes not - on institutions whose jurisdictions are often constrained by them.
- Finally, there is the increasing propensity of private citizens, organizations and nation-states to see cyberspace as a means of collaborating, competing, or engaging in conflict – activities that in previous times would have played out across physical geography employing traditional instruments of personal, soft or hard power. As with the other trends I define here, this trend can have effects perceived as good or bad. More importantly, the ubiquitous nature of cyberspace has made it increasingly likely that cyberspace will serve as the preferred venue for reconciliation of perceived disparity(ies) in the world – whether those disparities are in wealth, knowledge, or national interest. Witness the denial of service attacks by Iran on US financial institutions in 2012-2013, the attack by North Korea on Sony pictures in 2014, and the information war conducted by Russia against the US election process(es) in 2016.

The role of cyberspace as an essential foundation for personal pursuits, commerce, delivery of services, and national security combined with its use as a new geography, an alternative means for social organization and as a venue for reconciliation all converge to yield the challenges we experience on an almost daily basis. But because the challenges result from far more than technology and other phenomena within cyberspace itself, any attempt to address these larger strategic challenges will need to consider and address more than cyberspace itself.

To be more concrete, cyberspace may be considered as the sum of technology, people and the procedures and practices that bind the two. Any attempt to improve the resilience and integrity of cyberspace and the strategic things that depend on it must necessarily address all three and must, to the maximum extent possible, be constructed to work across physical borders as much or more as within them.

- By way of practical example, an organization desiring to improve the resilience of its information technology enterprise would do well to spend as much time and energy defining roles, policies and procedures as on the firewalls and security tools intended to comprise a defensible architecture. A review of cyber breaches over time clearly shows that failures in these procedures and human error are the principal weakness(es) exploited by cyber criminals, nation-state actors, and hacktivists.
- So, while technology must play a role in reducing the probability and impact of human error, vulnerabilities attributable to the human element will never be removed.
- In the same vein, governments must acknowledge that the globally interconnected nature of information systems and look for ways to craft laws and rules that will not be rejected by neighboring jurisdictions at some physical border, resulting in balkanization of systems and commercial markets, resulting in market inefficiencies, reduced system performance and security seams.

Some thoughts on essential elements of a solution follow:

Given the convergence of technology, the actions of individuals, and the collective actions of private and nations-state organizations that takes place in and through cyberspace, a bias for collaboration and integration must underpin any solutions intended to improve collective resilience and reliability. This calls for active and real-time collaboration, not simply divisions of effort, between the private and public sectors.

Analogous to security strategies defined in and for the physical world, the most effective solutions for cyberspace will leverage the concurrent and mutually supporting actions of individual actors, the private sector, the public sector, and government coalitions.

The private sector remains the predominant source of cyber innovation as well as the majority owner and operator of cyber infrastructure. The private sector must therefore be empowered and accountable within the limits of its knowledge and control to create defensible architectures and defend them. While the Cyber Security Act of 2015 made an important down payment on the ability of private sector organizations to share cyber threat information, greater attention should be given to increasing the incentives for private sector organizations to share and act on time-critical information in the defense of their data, infrastructure and businesses.

Government efforts must be biased towards the defense of all sectors, vice the defense of its own authorities and capabilities alone (an extension of the so-called “equities problem” that has traditionally focused on sharing information on inherent flaws in software and hardware). Government information regarding threats and threat actors must be shared with affected persons and parties at the earliest possible opportunity with a bias to preventing the spread of threats rather than explaining-in-arrears the source and attribution of already experienced threats.

The recent creation of the United Kingdom's National Cyber Security Centre (NCSC) represents a useful example of this approach. Comprised of about several hundred government experts from GCHQ (the UK's counterpart to the National Security Agency), subject matter experts from private sector organizations, and integrees from various civil and military UK government organizations, the NCSC's charter is to effect near-real-time collaboration between the private and public sectors, with an emphasis on the exchange of heretofore classified information. The resulting bias is to share without precondition, treating information as sharable by default, vice by exception. While the processes internal to the NCSC are worth examining, the transformation of private-public model for collaboration is the bigger story.

Uniquely government authorities to conduct intelligence operations, negotiate treaties, define incentives, and employ inherently governmental powers (criminal prosecution, financial sanctions, military action among them) must be employed as a complement to private sector efforts, not independent of them. A bias towards collective action by like-minded Nations will enable their respective private citizens and commercial organizations to optimize the conduct of their pursuits in and through cyberspace.

Whole of government approaches will, over time, define the various circumstances where cyber offense, an inherently military capability, should be considered and employed. In this vein, offensive military cyber capability must be considered as a viable element of cyber power, neither the most preferred or the tool of last resort. The extreme conservatism of the US government in its use of cyber offensive power in the past has not been met with similar restraint by its principal adversaries and has retarded the development of operational capacity needed to deter or counter ever more aggressive adversaries. That said, cyber offense should be viewed as an extension of, rather than an alternative to, cyber defense, most practicable when it rests on a solid foundation of defensible architectures and the vigorous defense of those architectures.

While uniquely challenging, the deterrence of adversary misbehavior in cyberspace can be significantly improved. Improved resilience and vigorous defense of enterprise infrastructure will aid in deterrence by denial. Improved attribution and vigorous pursuit of adversaries who violate defined norms will aid in deterrence by cost imposition. Collaboration across private/public and international boundaries will improve yields in this arena.

And most important of all, it should be remembered that no capability, across the private or public sector, is inherently tactical or strategic. Strategic objectives set the stage for strategy. Capabilities and tactics only have meaning within that broader context.

To that end, the actions taken by Russia in 2016 against various facets of the American election system must be considered in the context of Russian objectives and strategy. When viewed as such, Russian actions were neither episodic nor tactical in scope or scale. The lesson for us about the role of strategy and proactive campaigns in identifying and harnessing diverse actions to a coherent end-purpose is clear. While we must not compromise our values through the use of particular tactics against potential or presumed adversaries, simply responding to adversary initiative(s) is a recipe for failure in the long-term.

We must define and hone our strategic objectives. Strategy must then allocate those objectives to the various instruments of power available to us. Our efforts will be most effective when reinforced by alliances and when fueled by the cross-leveraging effects yielded by the concurrent application of individual, private sector, public sector power where offense and defense complement rather than trade one another.

Finally, in as much as I describe a mandate for government action in this space, I think government action must be:

- Fully informed by the various interests government is formed to represent;
- Focused on ensuring the various freedoms and rights of individual citizens while also maintaining collective security;

and

- Mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government both in facilitating the creation of an enduring, values based, framework that will drive technology and attendant procedures to serve society's interests, and in reconciling that framework to-and-with like-minded Nations in the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preferences of other nation-states which will drive, unopposed, solutions that we are likely to find far less acceptable.

In that spirit, I applaud the initiative and further work of this committee in taking up the matter and working through these difficult issues.

I look forward to your questions.