Speeches

"Confronting the Cybersecurity Challenge" - Keynote Address by Glenn S. Gerstell, NSA General Counsel

2017 Law, Ethics and National Security Conference at Duke Law School

February 25, 2017

Good morning, and thank you for having me at this impressive conference. I'm happy to be back here at Duke. I've had the pleasure of visiting the school on several occasions, including for recruiting for my former law firm as well as attending a wedding of a good friend at the Duke University Chapel. And back at NSA, we are delighted to have two fantastic members of your class of 2012 with us in the Office of General Counsel and we are looking forward to having another recent graduate join us this fall.

Yesterday, you heard from many experts on the topic of cybersecurity, which is a timely theme for this conference. Right now, that topic is at the forefront of American minds: there has been a proliferation of high-profile intrusions against U.S. companies, and malicious cyber activity will forever be associated with the 2016 election cycle. While I can't say I have the same qualifications as some of yesterday's exceptional speakers, I would like to talk to you today from my vantage point of not only a lawyer who spent many years in the private sector counseling companies around the world, especially in the telecom and technology sectors, but also -- and more importantly for today's purposes -- as the General Counsel for the past year and a half of the National Security Agency.

Now, many of you may be wondering why the General Counsel of NSA has decided to speak to you today at all -- indeed, for its first few decades the Agency's very existence was officially denied so there was no question that anyone on behalf of the Agency would ever speak in public. Fortunately that's all changed. But you might be expecting me to talk about surveillance rather than cybersecurity. After all, in the wake of the Snowden disclosures, most

people associate NSA with spying. Foreign surveillance -- or "signals intelligence" to use the precise term -- is, however, only half of our work. The other half, which is increasingly significant, is information assurance. In common terms, information assurance involves protecting and perhaps defending information and information systems. Our specific charge is to protect and defend national security systems, which include all classified networks along with those unclassified networks that involve intelligence activities or equipment that is critical to military or intelligence missions. So that includes all of the Department of Defense's networks around the world, and such specialized networks as the President's nuclear command communications system. This aspect of our mission, though somewhat unheralded, is of critical importance.

NSA is uniquely positioned to make key contributions to the nation's cybersecurity because, through its two missions of foreign surveillance and information assurance, it lives on the cutting edge of the global information space. Those twin missions complement each other in a way that enhances the agency's ability to detect and prevent cyber threats. NSA employs experts in signals intelligence, information security, and computer network defense and exploitation, and as a result of this expertise, NSA has end-to-end insights into malicious cyber activity, internet infrastructure and networks, the activities of hostile foreign powers, and cyber best practices. Although significant cybersecurity expertise resides elsewhere in the federal government, NSA is often regarded as possessing the leading collection of information security talent in the U.S. government based on the sheer breadth and depth of our focus on the subject.

So this morning I want to use that platform - informed by our twin missions - to explore new strategies for the organizational structure that underpins U.S. cybersecurity. I know that everyone here is a disciple of national security law, and as a result, this audience is more cognizant than most about the cyber threats we face today. But I will spend a few minutes just to make sure we all have a clear picture of the current scope of the threat, how we are currently postured to address that threat, and where gaps remain in that approach. I would then like to explore with you some thoughts on how our federal government should organize itself to address those gaps.

You hardly need me to point out the ever-increasing dependency on connected technologies in our everyday lives. In fact, I bet about quarter of you have already checked your cell phones since Major General Dunlap introduced me...maybe even half if my skills as a speaker leave something to be desired. The increasing interconnectedness of our networks and devices enhances convenience in an astounding way -- it's nice to know that I can use my smartphone to order an Uber car around the world and also adjust the water temperature of my home spa -- but along with that convenience -- for individuals as well as businesses and governments and other organizations -- comes heightened vulnerability. The vulnerability can take many forms. It wasn't that long ago that cybersecurity simply meant deleting emails from a Nigerian prince who needed your help in making a bank deposit. Beyond basic email hygiene, there are threats to an entire network - true, the network owner can take extra precautions to secure the network, but that security can be undermined by the one user who connects to it with an infected device or downloads a spearfishing email. Network threats by

definition can be as serious as the criticality of the infrastructure or equipment controlled by the network or the sensitivity of the information conveyed by the network.

A great deal of time and attention has already been spent assessing today's cyber threat. Study after study has echoed the gravity of our country's cybersecurity vulnerability. Experts agree that the threat is so grave because barriers to entry are extremely low while potential rewards are great, and the risk of getting caught for mischief is low. Malicious cyber tools are cheap and widely available on the internet. One lone actor with few resources now has the power to wreak havoc on a network anonymously. Cyber crimes are notoriously hard to track, and attribution can be challenging at best. These same studies typically put malicious cyber activity into one of three categories: cyber crime, in which criminals are seeking money outright...or something of value to resell, such as credit card numbers, tax IDs, and social security numbers, or they hold corporate data for ransom. Another category is cyber espionage. This category typically involves nation states, and it includes both political espionage and espionage for commercial gain, like the theft of trade secrets for economic advantage. And third, there's just general cyber mischief. This category includes hacktivists, those who use cyber vulnerabilities to spread propaganda, like ISIL, and those who seek to disrupt services or sites, like the recent DDOS attacks facilitated by Internet of Things botnets on the website of cybersecurity journalist Brian Krebs and on Dyn, a domain name service provider, that took down popular sites like Twitter, Spotify, and Reddit. And it's only a matter of time before this category also includes the deletion or alteration of data -- just think of the havoc that can create, especially in the case of the latter, where the malicious action might not be apparent.

So we know the nature of the threat -- and to give some sense of the scope of it, it's no exaggeration to say that cyber vulnerability is one of the biggest strategic threats to the United States. I was alarmed when at the first annual threat assessment I had the privilege of attending before the Congressional intelligence oversight committees, the Director of National Intelligence placed *cyber threats* ahead of *terrorism*. There are 23 victims of malicious cyber activity per second according to a 2016 report from Norton, and the Center for Strategic and International Studies recently estimated that such activity costs our *national* economy $140 billion each year. By comparison in just economic terms - and I don't mean to suggest they are really equivalent Â- the Institute for Economics and Peace, which publishes a yearly Global Terrorism Index, estimated that the *global* economic impact of terrorism was about $90 billion in 2015. And in case you were worried about the stock market bubble, the Chair of the SEC last year said that the gravest threat to the American financial system was cyber. The threat is so grave, in fact, that former CIA director and Secretary of Defense Leon Panetta described our nation's cybersecurity weaknesses as amounting to a pre-9/ 11 moment.

But surely we're doing something about it? Although the Bush Administration took steps to address cybersecurity policy on a national level, for example through the issuance of National Security Presidential Directive 54 in 2008, the issue remained somewhat obscure -- and indeed a year later the topic wasn't even mentioned in President Obama's inaugural speech. Over the ensuing eight years, however, as the topic rose in national prominence, the Obama administration took significant steps to implement a whole-of-government approach to

dealing with the multi-faceted cybersecurity threat, , including through issuance of PPD-41 and Executive Order 13636. The first laid out the framework for the US government's response to significant cyber incidents; the second provided a risk-based approach for managing cybersecurity threats. Executive Order 13694, also issued by President Obama, enabled sanctions against malicious cyber actors. He used this new Executive Order to issue sanctions against various nation state cyber actors, including against North Korea after the Sony hack and, most recently, against Russia for its cyber interference in the U.S. election. The Administration also authorized highÂ profile prosecutions of nation state-sponsored cyber actors. For example, the government indicted five Chinese military hackers for espionage against U.S. nuclear, metal, and solar companies, and it also brought charges against seven Iranians working for the Islamic Revolutionary Guard Corps who carried out intrusions against the U.S. financial sector and a dam in New York.

In addition to these Executive Branch efforts, and after much debate, at the end of 2015, Congress passed the Cybersecurity Information Sharing Act, or CISA, which is designed to improve cybersecurity in the U.S. through enhanced sharing of threat information between the public and private sector. Unfortunately, I don't think anyone believes that CISA by itself is adequate to the task. The statute's slow development was perhaps an indication that at the time CISA was being debated, the full scope of the cyber threat had not yet sunk in for all parties to the conversation and also, perhaps, that concerns about government surveillance remained high in the wake of the Snowden disclosures.

To further advance the discussion, the last Administration created a Commission on Enhancing National Cybersecurity, which recently issued its report containing some useful recommendations to enhance the government's cybersecurity efforts. Others, including think tanks, commissions, commercial companies, and professors, have also studied the problem and contributed proposals. To date, however, political will has not yet coalesced around one preferred approach, and the US government's response to cybersecurity challenges remains largely reactive.

Perhaps that is because, as many critics have noted, cybersecurity roles and responsibilities are unclear. Currently, cybersecurity responsibilities are shared across several federal departments, agencies, and congressional committees. To start off with, there are no fewer than six Federal cybersecurity centers â€“ the National Cybersecurity and Communications Integration Center (NCCIC) run by DHS, the National Cyber Investigative Joint Task Force (NCIJTF) led by the FBI, the Cyber Threat Intelligence Integration Center (CTIIC) housed within the Office of the Director of National Intelligence, the Department of Defense's Cyber Crime Center, US Cyber Command's Joint Operations Center, and NSA's own Cybersecurity Threat Operations Center (NTOC). NSA itself sits at one extreme of the operational model, with NSA being responsible for securing national security systems. That means, for example, that NSA is authorized to review and approve all standards, techniques, systems, and equipment related to national security systems. NSA also gathers foreign cyber threat intelligence and works to determine attribution of malicious cyber intrusions. But even for national security systems, however, there is no end-to-end solution. Within the Department of Defense, in which NSA is housed, there are procedures in place for enforcing network security standards

and best practices for national security systems. For national security systems outside DoD, however, those procedures are less robust because the network owners â€“ namely the other federal agencies -- have more autonomy and varied resources.

Contrast that operational model with the more advisory model that is used to protect the "dot gov" domain, which is overseen by the Department of Homeland Security. That department is responsible at least in principle for securing the remaining entirety of the federal government's networks along with critical infrastructure, although in reality each government agency has a major share of that responsibility. The National Institute of Standards and Technology, or NIST, which is organized under the Department of Commerce, develops the mandatory standards and guidelines for federal agencies' information systems. DHS is also principally responsible for communicating and coordinating in the cyber arena with the private sector, but nowhere in the federal government is there any meaningful authority to regulate, police or defend the private sector's cyber domain. Such authority as there is, is dispersed among not only DHS, but also various federal cyber centers that have been established, such as the Cyber Threat Intelligence Integration Center, and such disparate agencies as the Federal Trade Commission -- which has an important role in, for example, seeing that private entities safeguard consumer information from cyber data breaches -- to the Securities and Exchange Commission, which among other things regulates cyber protection for our nation's securities exchanges and registered stock brokers. And let's not forget the role of the Secret Service, which has a key role in combating cyber crime involving our banking system.

I could go on, but you get the idea -- cyber responsibilities are scattered across the federal government. To be sure, there are understandable reasons why it evolved this way and some good reasons for continuing a multifaceted approach at least in part. With the multiplicity of agencies involved, it's no surprise that simply coordinating incident response is a major undertaking. PPD-41 lays out a framework that assigns responsibilities for federal cyber response among FBI, DHS, and the Office of the Director of National Intelligence, but as you might expect, no one really thinks this is an optimal solution. And on Capitol Hill, while Congress has been active in holding many informative hearings over the past few years on aspects of the cyber threat, almost any Member of Congress (not to mention many outside commentators) would bemoan the fact that jurisdiction over cyber is spread among many committees and subcommittees - leading some Senators and Representatives within the past year to push for the establishment of a single committee to oversee cybersecurity.

In short, we can all agree that glaring gaps remain in our nation's cybersecurity posture. Former Secretary of Commerce Penny Pritzker correctly pointed out that "Even though the Internet is now ubiquitous in our lives, cyber remains the only domain where we ask private companies to defend themselves against Russia, China, Iran, and other nation states." For physical threats to the health and safety of our citizens, we do not ask each person to stand up their own personal Army, Navy, or National Guard - and for good reason. If dozens of Target or Home Depot stores were physically attacked, all at once, across the United States, the government would not stand by and hope that their own contracted security guards both repelled the threat and then healed the victims. Indeed, we are finding out seemingly every

day that we are vulnerable to cyber intrusions in ways that we didn't expect. The recent reports about hacks of political institutions with an intent to influence the Presidential election reminded us that just because a network does not fit within the definition of a national security system or fall within the sectors designated as critical infrastructure does not mean that it isn't a vital component of a fundamental American institution.

In addition, under the current structure, the private sector in general continues to have little to no incentive to concentrate resources on cybersecurity. Admittedly, there are companies in some sectors, such as finance, where the value of the product or service is intrinsically network-based, which do regularly share cybersecurity information and have sophisticated cybersecurity efforts. For the most part, however, private companies are incentivized to rush new products to store shelves in an effort to capture market share, and generate profits for shareholders. Delaying a product's release in order to assess and upgrade its cybersecurity can cost a company dearly, particularly if its competitors have not taken similar care. Many companies are even reluctant to share too much information because of concerns about protecting trade secrets and perceived antitrust collusion. It's by no means clear that the average consumer picks products and services based on a solid understanding of the comparative cyber risks present. That may be attributable to a lack of consumer education, or a conscious choice to weight other factors in product selection higher or industry's unwillingness or inability to address the risks - or all of these factors and others as well. But no matter what, it's incontrovertible that we do not yet have fully developed standards or practices in place that cause private companies in general to ensure the products they are selling are secure.

My purpose in reviewing the nature of the cyber threat is not to browbeat you with the severity of the problem, which I am sure you accept, but instead to implore you to join me in the conviction that the time to act is now. The incessant and rapid pace of technological development in the cyber arena continues to outstrip our ability to organize ourselves to address cyber threats before they become major cyber incidents. Some of the factors that might have contributed to our slow or tepid response to the threat -- ranging from lack of awareness to an unrealistic hope that somehow a public-private partnership would miraculously evolve to address the problem - have dissipated. We don't need to study or admire the problem any longer. Presidential elections have often served as the springboard for national initiatives and the new President has already signaled a strong awareness of the threat and an intention to do something about it. Moreover, interest in cybersecurity is high in the wake of the Russian malicious cyber activities, and the public is now more familiar with the role of intelligence agencies in protecting the national security. A major undertaking for the new Administration and Congress will be to take a hard look at the nation's cybersecurity and formulate a long term approach in an attempt to prevent a cyber equivalent of 9/ 11 -- one that simultaneously addresses both organizational obstacles and the underlying legal framework.

So let's turn to what should be done. As I've already alluded to, there has been no dearth of strategies proposed to address the cyber threat on a national level. They range from a recent Center for Strategic and International Studies report (advocating for making cybersecurity an

independent operational component at DHS while also strengthening other key agencies), to GWU's Center for Cyber and Homeland Security (recommending the development of a framework that would allow technologically advanced private entities to engage in level of proactive cybersecurity measures that fall between traditional passive defense and offense). Separately, the Presidential Commission on Enhancing National Cybersecurity recommended, among other things, improving public/private partnerships and increasing use of the current Cybersecurity Framework laid out in Executive Order 13636. Meanwhile, Representative Michael McCaul, the Chairman of the House Homeland Security Committee, has been working to pass a bill that would codify certain cybersecurity authorities at DHS's National Protection and Programs Directorate, which would be renamed the Cybersecurity and Infrastructure Protection Agency.

As you can see, much attention has been paid to the nation's cybersecurity, but a consensus has not yet developed regarding the preferred approach. What's revealing, however, is that virtually all of these studies seek to advance two overarching goals: *integration* and *agility*. Any new approach to cybersecurity must be integrated, in that it must include major national-level structures in which all divisions of government know their roles in clearly defined, non-duplicative assignments appropriate to the particular expertise and position of the government entity. Integration isn't merely a governmental imperative. A national coordinated solution by definition must involve both the public and private sectors, and equally must take full advantage of the intelligence and insights generated by our national security apparatus. Most importantly, it must coalesce around a national will -- the creation and sustaining of that should be the work of not only the executive and legislative branches but also corporate America and academia.

A new framework must also be agile. From my position at NSA, I've witnessed the challenges in sharing classified threat indicators within government and across the private sector, and I've also seen firsthand that the process for determining who can act and what approach should be taken in response to a cyber threat is slow and cumbersome, involving formal requests for assistance, several layers of approval, and time-consuming fiscal considerations. It is akin to calling county water officials when your house is on fire, who must ask for assistance from the fire department, which must then receive approval from the mayor and money from the city treasury before a truck can be dispatched. By the time this administrative legwork is complete, our cyber house has been reduced to cinders. It is essential that our cybersecurity framework be equipped with both the resources and the authority to anticipate, protect against, and respond to cyber threats with the speed that will make a difference.

So how do we accomplish this? One obvious and affirmative strategy, and the one that I think may have the most potential for achieving real gains, would be to unify the government's cybersecurity activities by establishing a new lead department or agency for cybersecurity. Easily said perhaps -- but exactly how would one go about doing it? Well, much as we did two centuries ago, we can again look to our neighbors across the pond for ideas. The United Kingdom faces the same cyber threats we do, but for a variety of reasons one could speculate on (perhaps having to do with their size, institutional strengths and political culture), they

sometimes are able to achieve solutions more quickly than can our arguably more fractious democracy. The UK within the past few months has selected a new integrated model, by creating the National Cybersecurity Centre or NCSC. Like the U.S., the UK had various entities, all with disparate responsibilities for cybersecurity. Their new center brought together and replaced four different entities. The NCSC is intended to act as a bridge between industry and government, providing a unified source of advice, guidance, and support on cybersecurity and management of cyber incidents. In other words, the NCSC model is intended to address both prevention and remediation of cyber threats and incidents by pulling together under one roof the full range of critical cybersecurity functions, including research, advice and guidance, and incident response and management. I am not necessarily proposing this precise model as the solution; after all, the UK has, as I noted a moment ago, a different culture, it is smaller, and the actual details of its legal system are quite unlike ours despite being obviously erected upon similar concepts. It is still useful, however, to examine the ground that they've started to break to determine whether there is anything that we can and should import.

The understanding that victims of cyber attacks were receiving conflicting advice and views depending on the government agency to which they turned was a major rationale for the UK to establish a unified cyber center -- but what really kick-started the UK to action was that the realization that relatively unsophisticated cyber intrusions, such as the attack against TalkTalk, a UK telecom provider, by a teenage boy, were turning into national level events because of a lack of basic cyber hygiene and because the government was not appropriately transparent about cyber threats and intrusions. Increased information sharing alone, however, was not the answer; UK experts decided that a more interventional approach was required in order to create consistency and coherency.

The UK carefully considered whether to organize the NCSC inside or outside the intelligence community. Much like in the U.S., there was apprehension in the UK after the Snowden disclosures about the role of its intelligence apparatus. Ultimately, however, the UK elected to stand up the NCSC as an agency wholly within the Government Communications Headquarters, which is the UK's version of NSA. This was done because, as I mentioned previously with respect to NSA, GCHQ already had the technical expertise and the intelligence insights that would be needed by the new organization. In order to overcome the public's apprehension, the NCSC committed itself to transparency: it publishes comprehensive data on cyber threats and, whenever possible, includes supporting evidence. Its facility is largely unsecured, so that it can bring in subject matter and technical experts from the private sector to teach NCSC personnel about their industries.

In conjunction with the establishment of the NCSC, the UK also rolled out its comprehensive National Cyber Security Strategy, which sets out the UK's approach to tackling and managing cyber threats to the country. It advocates for developing an innovative cyber security industry and provides for an active, nationwide cyber defense program. As an example, they've begun deploying a web check service, which scans for web vulnerabilities or misconfigurations in the websites of all public sector organizations in the UK. Website owners are provided a tailored

report about any issues identified. Overall, the UK has committed to investing over $2 billion over the next five years to transform their cybersecurity posture.

Naturally, there are drawbacks to a model such as the NCSC. For example, concentrating cybersecurity responsibilities in one lead agency misses an opportunity to marry cyber expertise with the unique insights and understanding of requirements possessed by each agency in their own fields. In addition, as we've seen with the Department of Homeland Security, there are always bureaucratic and political issues associated with standing up a new national organization. The potential advantages of this approach, however, seem for the UK to outweigh the disadvantages.

Could we do the same thing here? At least on its face, this could satisfy the two principles I suggested a minute ago -- namely, integration and agility. Most importantly, through unification, the cyber protection mission would be informed by the foreign intelligence mission that uncovers malicious cyber activity from nation states and political groups adverse to us. The benefits of that proximity are precisely what led NSA, in an internal reorganization last year, to combine its information assurance teams with the signals intelligence ones in a combined operations directorate. And in a slightly different but still highly relevant context, the decision to co-locate and partially integrate the new US Cyber Command with NSA was a critical factor in seeking efficiency and synergy for the new organization. If we were to follow the UK model, cyber security would be the principal mission for a newly-created organization, rather than a secondary or tertiary support function, as it currently is for many federal agencies, and it stands to reason that that focus would yield better outcomes. Unifying cybersecurity responsibilities in one organization would enable the federal government to eliminate redundancies and to concentrate and streamline cybersecurity resources and expertise -- both of which can be hard to come by in an era where the cost of purchasing and updating equipment and retaining cyber talent creates challenges to the implementation of cyber best practices. And manifestly, housing the cyber threat discovery, protection, defense, and remediation capabilities in one entity would afford the agility and timeliness that is critical to an effective cyber strategy. In short, I think the case for such a unified, central approach is fairly compelling.

Even if we all concurred that such an approach was the right one, there would still be many details to be worked out. One key question would be how to sufficiently empower the new organization so that it could effectively defend the various networks of many federal entities -- which would include the power to, in some sense, police those networks, setting and enforcing standards, perhaps even shutting them down if needed -- while at the same time letting each entity have some authority and responsibility for its own unique operations. A unified and nationally prioritized budgetary authority would clearly be a critical component of such an approach. Similarly, Congress would need to embrace this approach on multiple levels, including centralizing to some significant extent the jurisdiction over cyber matters that is now accorded to many committees and subcommittees. The very process of deciding what we are going to do, however, will require us to face these questions head on. This exercise will be valuable in forcing us to decide how cyber responsibilities will be shared across the

government, how the public and private sectors should work together, how to enforce compliance with standards, and how to respond to malicious cyber actors.

If this nationally unified approach were adopted, I am not necessarily proposing that such an organization fall within NSA. Although that is certainly worth exploring, we recognize that there are very real concerns about the scope of government surveillance and the potential use of "zero-day vulnerabilities" or cyber vulnerabilities that could be discovered by the government -- but at a minimum, NSA should have a special relationship with any new cybersecurity organization. It would make no sense to deny such a new organization the insights and warnings about cyber threats developed by NSA through its foreign intelligence mission. That would fly in the face of the very need for integration and agility. Whether that relationship takes the form of, for example, some deeper partnership between NSA and truly integrated cybercenter in a new Cabinet-level Department of Cyber, or housed, say, within the existing DHS, is something that the executive and legislative branches will have to sort out.

I want to make clear that by advocating that we avail ourselves of the infrastructure already paid for with taxpayer dollars and of the expertise and position of NSA, I am not, however, suggesting that NSA be granted additional surveillance authorities. We recognize that -- while increased communications monitoring might be an inevitable byproduct of confronting the cyber threat -- it's equally true that monitoring and implementing other technological approaches are fraught with understandable concern about government intrusion. Undoubtedly, there are portions of the population with unanswered questions (or worse) about us, but just because that perception exists does not mean folks like me are doomed to silence. Instead, I feel like we owe it to ourselves and to the public to enter the debate on topics like cybersecurity. The cybersecurity threat is grave, and we've got the unique expertise needed to help safeguard the nation against those threats. It's important to share some of our knowledge, developed over many years, in order to foster a vital public debate about the right way to address threats to our national security, and part of that debate includes an honest discussion about the pros and cons of locating a lead cyber agency or department within the intelligence community.

We at NSA feel duty bound to discuss these types of issues, and we'd like to do so transparently and openly to help reach a consensus as to the best approach. I hope that I've done that here today. Thank you for listening, and since I just spoke so highly about fostering discussion, I'd like to open up the floor for a few questions in the time remaining.

Date Posted: March 2, 2017 | Last Modified: March 2, 2017

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu