DRAFT: Annual Cybersecurity Summit

June 6th, closing Keynote

Summit Focus: "Human-Machine Teaming & Innovation Yield Mission Success "
This theme is about the ongoing artificial intelligence revolution and the incredible potential when machine learning is applied as a tool to assist human decision-making

---

Opening introduction- NSA- Short description

- NSA has two missions: Foreign Intelligence and Cybersecurity
- We develop foreign intelligence through analyzing signals. Signals Intelligence is the very essence of NSA's competitive advantage, as we work to discover threats and gain unique insights about foreign adversaries
- We learn what our adversaries are doing and we inform our military leaders, government partners, and policymakers to give them a decisive advantage in our nation's defense
- Second, we have a Cybersecurity mission. We leverage our cybersecurity authorities to test U.S. government networks and provide solutions to secure and defend National Security Systems and critical infrastructure, which handle the most sensitive data of the federal government and military
- We conduct system testing on Department of Defense networks by their request, either evaluating the security of their systems or performing penetration testing to measure the effectiveness of their team's responses to simulated cyber-attacks
- We advise customers and partners and we provide cybersecurity guidance to the public on how to protect systems, which is available on our website, NSA.gov
- We use those unique insights, expertise, and capabilities to help defeat the most sophisticated cyber adversaries targeting U.S. and allied networks

- Our goal is to proactively shape and counter our adversaries' experience in cyberspace. We both tactically counter the day-to-day malicious activity, while also strategically building campaign plans to support degrading and defending against our adversaries

---

Threat Landscape

- The threats to our national security are real, they are constant, and they are growing. When we are successful, the public never knows
- Extremists and international terrorists threaten our embassies, our military, our allies, and our homeland
- Regional conflicts pose serious threats to our national interests
- Hostile foreign governments, terrorist cells, and rogue individuals try to acquire weapons of mass destruction and/or the materials to produce them
- Last year's National Security Strategy highlighted the re-emergence of great powers in a revived competitive environment
- The National Defense Strategy prioritized and aligned DoD efforts for long-term competition with China and Russia (2) plus North Korea, Iran, Violent extremist Organizations (3) or "2+3"

Threats (Great-Power Competition)

- Today we are in an unprecedented level of challenge
- We're in a period of great competition
- For instance, while we want to maintain cooperation with China, they are doing everything possible to stay ahead of us in just about every area and keep us at a distance. China's rise to power is a great concern--economic power, military modernization, cyber capabilities; aggressively pushing technological and economic superiority
    - China has long-term cyber space goals that they have been operating through many administrations; A peer competitor intent on usurping us in Pacific Region
    - In many respects China has surpassed us in technological development

  - And they are leveraging this technology in pursuit of sophisticated targets with global ambitions, posing an unprecedented threat to the US, its interests through an emerging military force, economic power and influence
  - Their cyber threats, technology modernization, and global presence present a unique and formidable challenge
- Russia continues to sow division (internally and among allies) to weaken their political systems, will, and ability to act; they continue to use subversive measures to undermine America's credibility here and abroad
  - Over the past several years, Russia has taken a series of actions that demonstrate its desire to be recognized amongst the world's great powers and for global influence
  - It leverages cyber in two important ways, first as conditioning setting tactic in combination with offensive operations
  - Second, to mount significant, well-orchestrated and culturally specific misinformation and disinformation campaigns to undermine the foundational elements of our democracy
  - Additionally, Russia supports or harbors significant cyber-criminal activity affecting the US and its allies
- North Korea is rapidly advancing in the areas of cyber, nuclear and ballistic missile programs. We're very, very familiar with North Korea's capability, and certainly their intent. They've had both the capability and intent to strike our nation destructively in cyber space and will continue to try to improve their capabilities in cyber space
- The Middle East is still home to the most dangerous terrorist organizations and Iran is the world's leading state sponsor of terrorism
- Iran thrives on instability and continues to perpetuate the cycle of violence in the region

Threats (Dynamic/Changing Environment)

- Our adversaries do not share our values
- They are operating below the level of armed conflict through malicious cyber activities (stealing intellectual property, steeling personal

identifiable information, use of proxies to conduct malign influence in our elections and society)

- Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action
- Despite this dynamic/changing threat environment, we are uniquely suited to address these emerging challenges
- We have adapted and changed our approach to how we do business
- We have positioned ourselves to be part of the larger whole of government efforts to counter China, Russia, and Iran
- NSA is building and implementing comprehensive plans to overcome the very real threats to our country and continues to provide national decision makers with insights about what our adversaries are doing and what their capabilities are. We help them understand the adversary's activity so they can make decisions and plans, and execute policies and operations
- Information is power. When we know our adversaries' information and they don't know ours, we have the "Information Advantage "
- That "Information Advantage" is what NSA gives our customers – and our Nation

---

Competitive Advantage

- **Partnerships**
  - We have strong, significant partnerships across the IC and industry
  - We continue to forge new anew emerging partnerships that are mutually enabling with a goal of working with our partners to put the best player in the game—we get there as a team; at the time

of execution regardless of position, role, or squad we must put the best player in the game

- Foreign Partnerships
  - NSA has the most robust and complex array of bi-lateral and multi-lateral partnerships in the USG
  - NSA relies heavily on partnerships to enable or enhance our capabilities or to do things we simply cannot for a variety of reasons
  - Partners are providing access, capabilities, and accepting greater risk than ever before
- Interagency Partnerships
  - Incredible IC workforce – ref DIR's visit to NGA St. Louis
  - Unprecedented partnership and coordination during Russia Small Group
  - Enhancing partnerships: renewed focus on NRC positions, targeting talented personnel and elevating stature of these assignments
  - On path to expansion of a larger IC Information Environment
- Industry Partners
  - Industry partnerships are our asymmetric advantage in cyberspace
  - Despite "exposures" (2013-16), industry partnerships still very strong
  - Continued challenges in information sharing w/ partners (operationally)
  - Sharing is critical to building trust and transparency; must measure balance of benefit (us vs them) or creating competitive advantage
  - Sensitivity where industrial partnerships are concerned (legal risks)
  - Must leverage private sector/industry in area of cybersecurity
  - NDAA includes language to expand CIFIUS
  - Use of commercial cloud solutions
  - Movement to pull Microsoft Azure into classified domains

  - GREENWAY Program stabilize and standardize how we provide basic IT services around the world
  - We are a huge service provider, we are consumer of services from others that rely upon the services we provide (mutual dependency, mutual support)
- Overseers
  - Bi-partisan support to 702 (extended 6 years); three others will be considered this year
  - Continue to buy back and increase confidence (since 2013)
  - Accepted risk that we would be successful with RSG
  - Solarium – law, great opportunity, could be nothing, could complicate things for us
  - Good place, good relationships; leveraging returning fellows
  - Need to broaden interaction w/Judiciary Committees and others – continuous relationships vice episodic or in time of need
  - Recent activities in Congress indicate that "everyone" is involved in legislation related to NSA, not just SSSCI/HPSCI, SASC/HASC
  - Transparency is important, critical to our relationships; however, there is a one-way ratchet on reporting demands – only increase, expand, and continue to escalate and intensify – having considerable cumulative effects (time and resource burdens)
- Academia
  - Recently approved an Academic Partnership Strategy to complement the existing and mature NSA strategy
  - Maturing in new ways - beyond recruiting; expanding to problem solving & innovation
- Power of Integration – USCYBERCOM & NSA
  - Russia Small Group – partnership generated unprecedented and unexpected opportunities without imposing risk to enduring intelligence efforts and priorities
- Research
  - In addition to enjoying most robust and extensive partnership with DoE in our history...

- Our talented experts continue to innovate and make a difference not only in technological advantages Human Language Technology

- **Cutting edge technology and desire for constant innovation**
  - We are developing new strategies utilizing the Internet of Things
    - Collaboration with private industry will help ensure that security is included in IoT systems from the beginning
    - New attack vectors
  - We are leveraging technology and innovation to reduce our dependency on some jobs that could be enhanced with automation
    - Automation is necessary to help prevent single points of failure and reduce the dependency on certain jobs
    - Automation is critical to addressing threats in real time as AI becomes more pervasive
    - Enables NSA employees to focus on other core mission aspects instead of spending time developing new tools from scratch
  - We are at the doorstep of some major breakthroughs – and I don't think this is overstating it -- as a civilization
    - Advent of the Quantum Computer:
    - Functional quantum computers are arriving on the scene with examples from IBM, Intel, Google and others. While they are still nascent, the implications on security of our financial system, data protections, and frankly our national security interests are massive
    - We are working to understand the implications of this technology to both our Foreign Intelligence and Cybersecurity missions. It challenges us in all of our core areas of scientific, cryptographic, and mission expertise. These include:
      - Making new codes (encryption techniques) for the nation that are secure against quantum computers for long periods of time

- (U) Employing any new capability to help break the codes of the future and generate new insights for our nation's decision makers
- (U) Understanding the risk implications of this new "quantum world" to the data secured with algorithms designed before the advent of these new machines

- (U) Synergy of Machine Learning and Human Intelligence:
  - (U) Massive data generation and the need to generate insights from it has driven rapid development of machine learning technologies
  - (U) While that area continues to grow, we are also rapidly understanding the limitations of these algorithms and the additional workload that is being placed on human users when they don't work well
  - (U) In the cybersecurity mission, for example, we have seen and heard from our industry counterparts about the challenges associated with false-positive intrusion events reported by ML / Artificial Intelligence (AI) powered systems and the human resources they can consume
  - (U) The synergy of human – machine interface will be a powerful tool to achieve mission outcomes
- An example of how we are working together: NGA did unclassified development building a version of NSA's internal tradecraft hub tool. The intent of that is to allow each agency to document and intermingle its tradecraft so that we are answering questions consistently against the same types of data—that's innovation because in the past we were not able to talk easily about tradecraft, use cases, mission applications, and hard problems (example)

- **National – tactical integration**
  - We are working very hard to not only converge the data across intelligence agencies at the national level but working very hard to get our tactical partners data made available on both the

classified and unclassified networks for everyone to use—this data convergence is not limited to NSA and NGA partnerships;
    - Getting the building blocks into a cloud environment to allow us to ask large behavior based questions and automate analysis through analytics
- Speak of experiences at the ADF-C (my previous assignment) TechSIGINT & GEOINT

What's the Future Look like?

- Operating on a common geolocation foundation is critical:
    - Common data standards, interoperability, converged MULTI-INT data all geospatially indexed
    - Common IC usage of data / services, all working on the same facts, share of best practices in tradecraft across agencies
    - End goal of getting the information to the lowest possible classification so it can have the best outcome
    - Aggregating all of our data not only helps us improve the precision, but it helps us more fully understand the full global operating environment →partnership is never before more critical than it is now

AI / ML – automation – Cyber Defense, SIGINT, GEOINT

- As we converge our data and have a more holistic picture of our target operating environment things like AI and ML will play a big role—now instead of analysis manually review information, we are taking data driven approaches that allow us to better understand the patterns in the data that help the system work got the human and identify anomalies and what's normal and help us better characterizes the environment

Multi-INT tipping & queuing

- If one agency sees a pattern of interest we need to be able to automatically tip or initiate a response at other agency

Deepening our partnerships across the IC and rest of government, industry, & academia

- NSA works hard to support the warfighter who puts himself on the line every day for each of us Intelligence success only happens through collaboration, and partnering to operate on a common geolocation foundation is never before more critical than it is now
- There is power when agencies work together to solve hard target problems
- Each partner only see a part of the target space, and when we aggregate data, brain power, and analytic capacity, we can be a force multiplier to provide our combat support role
- Our approach is deliberate and fuses products for separate entities /authorities into dual-sealed product that presents a more complete and actionable picture
- Ultimate success comes down to having a common framework when we talk to each other—the same terminology, same data standards, similar tradecraft and approaches to understanding target environments;
- A common foundation and framework allows us to more smartly interact with each other as well as industry and academia because we are asking the right questions because we know what we have; we understand what each agency brings to the problem and we understand their approach, tradecraft and methodology; we're able to have more of an open, transparent conversation and realize where there is duplication and where there are efficiencies
- The dream would then be to ask industry and academia to help meet our gaps that are truly gaps—if we are not communicating and are talking past each other than we are not optimized or efficient— without this holistic approach we lack a comprehensive understanding of our posture and we could be asking for help with problems that have already been solved by a partner agency
- End goal of getting the information to the lowest possible classification so it can have the best outcome
- Aggregating all of our data not only helps us improve the precision, but it helps us understand the full global operating environment
- Partnership is never before more critical than it is now

Persistent innovation – dynamic threats require dynamic change – outmaneuver our adversaries

- The more we aggregate our tradecraft; the more we speak the same language the more that we have consistent converged data then we can have automation
- Automation will help us to be more dynamic and agile in response to threats
- Without Automation and we are trusting analysts to observe patterns and anomalies and we will never be able to maintain a strategic advantage to outmaneuver our adversaries

---

NSA's Geolocation strategy is working to achieve these high level outcomes:

- CONVERGENCE: User can leverage "all geolocation facts" in their mission use case
- ACCURATE: Meets combat support, legal, and analytic support requirements (resolution, speed, frequency)
- CONTEXTUALIZED: Users understand how the data relates to the target, collection, and network
- TRANSPARENT: User understands the type, value, and quality of the data, to include limitations (age), provenance, and confidence/trust
- MEASUREABLE: Monitoring metrics determine what is of value to users, and reports back to collection/data providers for further refinement and to inform investment
- SOURCEABLE: Analytic outputs are available to the warfighter
- AVAILABLE: Integrated & standardized into the users workflow, accessible to different types of mission use cases, training, and accessible at the lowest classification possible

---

Conclusion

- GEOINT enables us to apply SIGINT resources more effectively and track targets for situational awareness and discover new targets by detecting known patterns

  - We are focusing the conversation on analytic mission use case (e.g. Tradecraft hub) (AI/ML, ABI) to identify discovery opportunities from patterns in the data
  - We are developing innovative machine learning algorithms that our partners can adopt
- We do this through our strong partnership with NGA
  - The successful partnership has existed for years as evidenced in our joint reporting activities, we have an exciting future as we look at expanding into analytic tradecraft collaboration, looking at behavior based discovery of geospatial patterns of movement over bulk data
- Work together to leverage the expertise from both communities to assess threat and providing threat warnings
- SIGINT and GEOINT are the eyes and ears of intelligence—it's a success story: IC partners working together to focus on hard problems
- Our approach is deliberate and fuses products for separate entities/authorities into a dual-sealed product that presents a more complete and actionable picture—we ultimately need to be ready to react when/if something bad happens
- We're developing innovative machine learning algorithms that our partners can adopt
- Our continued goal is to get critical, actionable information to national decision makers and the warfighter
- Predictive analytics are key/logical network for physical integration of images and telecom data
- End goal of getting the information to the lowest possible classification so it can have the best outcome

What we need from the GEOINT Community:

- Help us make our corporate architecture operate successfully – don't build your own
- Comprehensive awareness of our capabilities for each priority target area, across all data types
- Only by data convergence can we have a truly holistic picture of the battlespace and target environment