The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

2015 AUSA Annual Meeting & Exposition

October 12 - 14, 2015 Washington, DC

Day 1

Threats in a Complex World

On Monday the CyberWire attended a panel on "Threats in a Complex World." The presentations provided a larger context for understanding international and transnational cyber conflict.

Lieutenant General Mary Legere, US Army Deputy Chief of Staff for Intelligence (G-2), chaired the panel, which included Dr. Nadia Schadlow (Smith Richardson Foundation), Mr. Patrick Prior (US Defense Intelligence Agency), Dr. Patrick Clawson (Washington Institute for Near East Policy), Dr. Phillip Karber (Potomac Foundation), Brigadier General Karen Gibson (Deputy Commander, US Joint Force Headquarters-Cyber), and Dr. Erin Simpson (Caerus Associates).

After quoting General Miley on the current US predicament, "lacking the luxury of a single opponent," Lieutenant General Legere noted that the audience would be familiar with how the Army sees the world, as unstable, with a complex threat spectrum. She would give each of the panelists an opportunity to discuss threats from the perspective of their particular expertise.

A Snapshot of the Latest Global Trends Threatening our World

Dr. Schadlow opened by providing a construct for how to group and understand trends. She presented these as a set of "asymmetries." "Asymmetry of will," in which adversaries show a determination to reduce US power and influence, weakening both assurance and deterrence. "Asymmetry of purpose," a variety of the attacker's advantage — it's easier to tear down than it is to build, and disruptive actors find it easier to achieve their aims than the US will find it to thwart them. "Asymmetry of local knowledge," which is particularly well-entrenched in US institutional practices that militate against getting and maintaining local knowledge. "Asymmetry of geography," in which US forces will, effectively, always be foreign to a theater of operations. "Asymmetry of agility," in which the right tools simply aren't in US hands. "Asymmetry of resources.," particularly in the willingness to deploy and use them. "Asymmetry of narrative" (especially in social media), and "asymmetry of borders," arising from enduring US state-centricity.

After reviewing the asymmetries that favor the adversary, Schadlow noted that the US does enjoy asymmetries of combined arms capability, allies, territorial security, and humanity, the last being a more deeply compelling, if less immediately appealing, set of fundamental values.

An Insider's View of the Magnitude and Scope of Foreign Terror

The US Defense Intelligence Agency's Patrick Prior offered an overview of global terrorism. He noted that three major terror organizations are currently fighting in Iraq and Syria alone, operating with hostility to the United States but at cross-purposes to one another. Thus, the terrorist world is enormously complex in its interactions among groups and states. "It's hard to

know where to push," since advances against any one threat group often tend to empower its competitors. It's difficult to find partners in an environment with many independent actors and competitors.

Continuing his focus on the Middle East, Prior described the principal effect of the Arab Spring as creation of instability exploited by terrorist groups now establishing themselves as competing authorities. This is consistent, he said, with the history of modern terrorism being closely tied to ungoverned space.

Both al Qaeda and ISIL have advantage of instability in effectively ungoverned space. These groups can be counteracted, Prior observed, but only with difficulty, and with great commitment. Consider that ISIL has collected eighteen affilliates over the last few months, even as they've been under attack from many other actors. "The Libyan affiliate is the one we now find more worrisome. And we still, of course have Al Qaeda," which may be down relative to ISIL, but cannot be counted out.

It would be a mistake to think that all terrorism, even all terrorism in the Middle East, has a radical Sunni inspiration. To take one recent case, an obscure communist group has recently conducted bombings in the region.

Prior turned to cyberspace in his discussion of terrorist information operations. These have proven particularly effective in inspiring (as opposed to directing) homegrown violent extremists. Terrorist propaganda is slick; it resonates with the susceptible, and its target audiences find it readily accessible, especially on the Internet. Such information operations have changed the way in which terror attacks are carried out. The big terror attacks we remember (Khobar Towers, the USS Cole, 9/11) were centrally planned and directed by senior terror leaders. But the lone wolf is a new development, and represents the new norm. Since February 14, we've seen thirty lone wolf attacks in Western countries. And we see the success of online propaganda and related information operations in the flood of foreign fighters to Syria.

As had Schadlow, Prior leavened his overwhelmingly grim presentation with a few hopeful notes. "There have been bright spots. We've pushed ISIL back 20-30% in Iraq. There's been progress against FARC." But he left a strong impression of the ongoing success of terrorist information operations and the supercession of direction by inspiration.

Iran: Domestic, Regional, and Global Designs

Dr. Clawson opened by pointing out an enduring ambiguity in Iran's identity: "Is it a country or a cause?" Iran hasn't yet decided, but the ambiguity has great implications for Iran's strategy.

Iran is extraordinarily different, culturally, from the US. (Clawson claimed on cultural anthropological grounds that Iran and Japan were the two countries that least resemble the United States.) We find, for example, Iran trying to undermine even friendly governments, as they tried to undermine the generally sympathetic Maliki government in Iraq. The Iranian government is close to Assad, but also supports and organizes Syrian rebel forces (which is why the Syrian regime is delighted to see the Russians arrive as a counterweight to the Iranians). The Iranians "bet on every horse in the race." Hostile on sectarian and other grounds to ISIL, yet Iran permits ISIL's principal fundraiser to live in Tehran. We Americans would regard this as strategic incoherence. Iran regards it as a sensible hedging of bets.

Another difference between Iranian and US strategic culture, Clawson argued, is that the US is interested in results, but Iran is interested in impressions. The point is perception, the ability to claim credit. Iran believes it gains a lot by being able to take a principled stand against "global aggression," that is, against the United States. In such matters results as Americans might conceive them frequently count for little. For example, the US destruction of the greater

part of Iran's navy is studied by that navy as a victory, because in the encounter Iran took a principled stand.

Americans place great importance on our declaratory policy. But no Iranian politician ever criticizes another for failing to follow declaratory policy. Rather, Iran values expediency and flexibility. Clawson cited the founder of the Islamic Republic, the Ayatollah Khomeini, who famously said that, to preserve the revolution, one could forego any given Islamic tenet. Clawson advised that fatwas we hear from Iran (noting in an interesting aside that oral fatwas are more binding than written ones) should be understood in this context. "A fatwa is not like a Papal encyclical that endures for centuries. Fatwas change."

These US-Iranian strategic cultural differences are not going away, Clawson said. They're rooted in a complex, ancient culture. Those running Iran are firmly convinced the US represents an existential threat to their civilization, and this threat lies in our ideas and the attraction of our culture. Iranian culture is profoundly influenced by ours. Iran's rulers recognize the attractiveness of American culture and correctly perceive it as a threat. They fear Hollywood more than Washington.

Clawson concluded, as his predecessor had, on a more hopeful note, and one that pointed toward the importance of information operations. Iran today is very different from what it was ten years ago. Many Iranians want to join the world. Yet at the same time the leaders of the Islamic Republic correctly recognize enduring US cultural and political opposition. We won't convince those leaders otherwise.

Examining Russia's Policy Near, Abroad, and Around the World

Dr. Karber's presentation was more devoted to kinetic threats and operations than were the other panelists' presentations. His overarching point was that, while we've been tempted to define Russian operations in Ukraine and elsewhere as "hybrid warfare," this is misleading. "Hybrid warfare" is our term, and we need to arrive at some clarity about how the Russians themselves understand their strategic, operational, and tactical arts. The Russians themselves call what they're engaged in "new generation warfare." His view of the extensive threat Russian electronic warfare poses should interest those aware of US dependence on networked systems.

He reviewed his observations of Russian capabilities in Ukraine, and it was striking how reminiscent those observations were of those made at the US Army's post-Vietnam nadir. He credited the Russians with extraordinary electronic warfare capabilities (including ability to disrupt the functioning of electronic artillery fuzes), the ability to rapidly deliver massive fired (in a ten to fifteen minute cycle). The US has emphasized precision, the Russians mass, and their forces now deploy unusually lethal top-attack and thermobaric munitions.

To summarize Karber's account, the 1970s are back, and the US Army needs to dust off its Cold War doctrine, rediscover artillery, and relearn how to deal with a very heavy EW/SIGINT threat.

A Look at Global Cyber Threats to Army Systems

BG Gibson began her presentation by recalling her recent opportunity to review the old days of electronic warfare for a group of young officers. She had come into an Army in which we did radio direction finding by applying protractors to maps. This world has changed out of all recognition — it's now completely alien to the current generation of junior officers. Young officers today cannot conceive a world without the ubiquity of cyber.

And indeed, Gibson said, it's impossible to overstate the importance of cyberspace. We depend on it in all other domains. "Our capabilities in cyberspace are great, but so are our corresponding vulnerabilities." Our adversaries use the same Internet and the same mobile

devices we do. They can easily find vulnerabilities. In contrast to former counters of national power, like nuclear weapons, cyber weapons are far less expensive and very easy to procure. Non-state adversaries now easily attain state-like capabilities.

When adversaries can hit us with very small investment, we find ourselves on the wrong side of the cyber economic curve. And these adversaries act not only against military forces, but against businesses, non-governmental organizations, and private citizens. At extreme end of this threat, we could face what's been called a "cyber-armageddon," a general attack against critical infrastructure that could disrupt delivery of power, water, and other essentials. But the much more likely scenario is a long-running campaign exacting cumulative costs over time.

Quoting Director of National Intelligence Clapper on how the cyber threat has become more diverse and more threatening, Gibson offered the familiar division of threat actors into states, criminals, and hacktivists.

She reviewed the principal state threat actors, Russia, China, Iran, and North Korea. Russia, she said, is the stealthiest, most sophisticated cyber adversary. And Russian cyber crime factors into this, as the state turns criminal elements to its advantage. OSINT suggests that China is most active in cyber espionage, especially industrial espionage and theft of intellectual property. Iran has shown itself most interested in computer network attacks, particularly distributed denial-of-service and destructive attacks, with the Saudi Aramco incident being the most well-known example of the latter. Finally, we saw the North Koreans active in the Sony attack.

Cyber criminals represent the second class of threat actor, and they are for the most part, obviously, motivated by financial gain. The third class of threat actor comprises the hacktivists. While these have typically been dismissed as a nuisance threat, they're becoming more dangerous.

Gibson concluded with a now familiar call for a "whole-of-government" approach that take due cognizance of the fact that the vast majority of critical infrastructure is in private hands. The Army and the Department of Defense must deepen their cooperation with industry and academia, and develop closer relations with our allies. Many thousands of Army systems depend on connectivity, but were developed before cyber threats were a matter of concern. In the future, redundancy, resilience, and reliability must be built into systems from the beginning. And we need an improved cyber culture. Most breaches come from user or administrator mistakes. The United States Army is already engaged in cyberspace, and defending it will require Army-wide effort with all network users on the team.

Which Technologies Most Challenge the Current and Future Force?

After a brief preamble in which she reminded the audience that technology is always developed and used by organizations, and that understanding technology requires understanding organizations, Dr. Erin Simpson talked about disruptive technologies. She invited all to consider two kinds of technology, that which enables you to continue to do what you're already doing, only better, and technology that enables you to do something new. The latter kind of technology is disruptive.

She finds that the threat to US interests comes principally from novel uses of existing technology. The democratization of technology forms part of a larger trend that privileges software over hardware. This development lowers barriers to entry. Rapid hardware change is tough, rapid software change much easier. Adversaries use democratized tools to achieve very traditional military objectives, only rarely to achieve truly disruptive ends. Non-state groups in particular are mimicking core warfighting functions.

There's a rich role for open-source collection in our current conflicts. We should, Simpson argued, look closely at improving OSINT. We should also remember that concept development is more important than weapon development: the organization of technology is the place where revolutions occur. She also noted that we're unlikely to find disruptive capabilties within the Department of Defense or even in the Defense Industrial Base. "Disruption is painful. It breaks rice bowls."

Question: "This has been depressing…"

A questioner asked, "Is there a time in recent history when people in the United States were less informed?" Karber took the question and answered unambiguously. "Yeah — following the early 1970s we were in a real downer." The 1973 War [the Yom Kippur War] challenged our assumptions. Historically, the US Army needs leadership who can do what Generals DePuy and Starry did for its doctrine in the decade before the Cold War's endgame.

Question: "Why won't Iran change?"

If, a questioner asked Dr. Clawson, many in Iran would be inclined to assimilate into Western culture, why won't Iran change? Clawson replied that his liberal Iranian friends are happy the anti-government riots against patently rigged elections a few years ago didn't succeed. The only good change will come from within. Iranian leaders are quite comfortable with sectarian war. His liberal Iranian contacts say they hate the Islamic Republic Governing Council, but at least (in an observation Thomas Hobbes would have understood immediately,)"the IRGC lets us sleep at night."

Question: Should US policy continue to avoid the religious dimensions of conflict?

Will violence committed in the name of Islam crest and be exhausted? And, in a related question, is US policy of staying away from religious dimension of conflict sound? Schadlow thought that the religious dimensions would continue, and that no, current US strategy isn't ultimately sound. Price noted that there's a war of ideas under way, and, while we have the better ideas, tactically we're doing a poor job of countering the adversaries' narrative. Clawson said that people, particularly young people, who turn to radical Islam are often only loosely connected to Islam. We need, he thought, better ways of letting young people express dissent.

Question: What's your over and under on Syria?

Could Assad have acted other than as he did? Clawson has been surprised by Assad: he thought Assad would fold. But Assad has successfully turned back the calendar several decades and restored an Alawite position that had long been in decline. Eleven million Syrians won't sleep at home tonight. That makes a society hard to rebuild. And few of the refugees will return. Assad has successfully conducted an ethnic cleansing.

Question: What about forward presence?

People invite us into unstable places, a questioner noted. Is there an argument for a return to forward presence? Karber again counseled relearning the lessons of the successful Cold War. He observed that, in his view, "The Ukrainians don't want to be like us. They are us. They want to be part of the West." Putin has alienated the Ukrainians for at least a century. Our Civil War stayed in our mind for a hundred years, and Putin's war will have a comparable effect. We need, Karber said, a forward presence in Europe.

Question: How optimistic are you about the Government's cyber posture as a whole?

Gibson anwered by noting the central importance of points-of-partnership. "We need to harness the power of Silicon Valley. I'm optimistic about this." She added that a whole-of-government approach (something we've always said we needed) is especially important to cyber. She see the difficulty of achieving such an approach fundamentally a problem of human capital. The Twentieth Century's approach to acquisition doesn't work in cyber, nor do the last century's approaches to training.

Day 2

Homeland Defense/Homeland Security: the Army/DHS Partnership

The Honorable Jeh C. Johnson, Secretary of Homeland Security, addressed the AUSA yesterday morning on partnership between the Army and the Department of Homeland Security. We offer an overall observation: clearly "whole-of-government" solutions and approaches are de rigeur everywhere, but this seems especially so when officials talk about the challenges of cyber security.

Secretary Johnson reviewed his connections to, and affection for, the US Army, on both a personal level and on the basis of his appreciation for the work the Army continues to do in support of Homeland Security.

The burden of his remarks on cyber operations lay in that region where intelligence meets information operations. "The global threat," he observed (and in this observation he's certainly not alone) "has evolved from terrorist-directed to terrorist-inspired attacks." The 9/11 was terrorist-directed. But this is no longer the norm. Instead, today we see the terrorist-inspired attacks carried out by home-grown actors. We see the lone wolves, the foreign fighters, in incidents like the Boston Marathon bombing, the Ottawa attacks, the Charlie Hebdo massacre, and the shootings in Chatanooga. "This is the new reality," he said. "The homegrown actor is much harder to detect."

That lone wolf is also harder to interdict. He's inspired by something he sees, and thus in many respects represents a more troublesome threat. So, while we continue to take the fight to terrorists overseas (and Secretary Johnson expressed some satisfaction in the success the United States has realized in killing Osama Bin Laden and either killing, capturing, or otherwise neutralizing other terrorist leaders), this is insufficient as a response to the terrorist-inspired actor.

He reviewed law enforcement responses to home-grown threats, giving much credit to the FBI. He cited the Department of Homeland Security's Countering Violent Extremism (CVE) program of outreach to Muslim communities. In his experience, Muslim communities see ISIS as hijackers of Islam, and those communities he says, "help us help you." The Department's new Office of Community Partnerships will lead CVE efforts.

In describing the Department's other cyber initiatives, he called out what he characterized as an "aggressive" plan to enhance dot-gov security, with an ambitious timetable to secure those civilian Government nets with the Einstein system.

He urged swift passage of pending cyber legislation, and had good things to say about both the House and Senate versions. The principal benefit he sees in such legislation is the encouragement of information sharing.

He closed with some praise for the recent cyber agreement between the United States and China (although only "time would tell whether the Chinese will live up to these undertakings," he expressed a hope for more international cooperation in cyberspace).

He ended on a familiar but important note recalling that security must be balanced against the price it exacts in liberty. “You could fully secure a city, but it would be indistinguishable from a prison.”

Day 3

The third and final day of the AUSA Annual Meetings closed with a long and informative panel on the state and future of Army cyber. But a highlight of the afternoon was Secretary of Defense Ashton Carter’s visit to the Cyber Pavilion. A number of speakers described the Secretary’s strong interest in, and commitment to, Defense cyber capabilities. His conversations at the Cyber Pavilion gave some immediate currency to those descriptions. He’s shown here in dialogue with Joe Billingsley, founder of the Military Cyber Professionals Association.

“Feedback from all sources clearly state that AUSA’s first Cyber Pavilion was a huge success for all involved,” Billingsley told the CyberWire. “It attracted a large and diverse cross-section of the American military cyber community. Many senior leaders spent quality time with us including Secretary of Defense Ashton Carter, former head of OSD Cyber Policy Major General (retired) John Davis, former Deputy Commander of Fleet Cyber Command Rear Admiral (retired) Bill Leigher, leader of the Cyber Patriot program Brigadier General (retired) Bernard Skoch, and Deputy Commander (Operations) of the 335th Signal Command Brigadier General Stephen Hager. There was also considerable participation by academic institutions like National Defense University and Silicon Valley partners like Adobe.”

A 501(c)(3) educational non-profit organization, the Military Cyber Professionals Association takes as its mission “To develop the American military cyber profession and invest in the nation’s future through STEM education.”

Countering Violent Extremist Threats to Army and DoD Personnel and Facilities

A panel moderated by Rear Admiral (retired) Don Loren took up the issue of violent extremism, and how it might be countered. Much of the discussion centered on the importance of training and close coordination with local law enforcement authorities. But of particular interest to a

cyber audience was the session's reiteration themes heard over the last two days, particularly in Secretary Johnson's address yesterday, and in Monday's panel discussion of Threats in a Complex World. The threat of violent extremism is a transnational one that's unmoored from traditional command and control. Today's terrorist is for the most part no longer directed, but inspired, and such inspiration reaches the lone wolves around the world through cyberspace. As cyber operations become part of the extremists' arsenal, any barriers to communication with civilian authorities impose significant risks on us. Any "whole-of-nation" solution needs to include state and local authorities.

Army Cyber — Today and Tomorrow

Moderated by New America Foundation Strategist and Senior Fellow Dr. Peter W. Singer, the panel featured Lieutenant General Edward C. Cardon, Commanding General, US Army Cyber Command, as its lead speaker. They were joined by Major General Stephen G. Fogarty (Commanding General, Cyber Center of Excellence and Fort Gordon), Major General Paul M. Nakasone (Commander, Cyber National Mission Force, US Cyber Command), Colonel William J. Hartman (Commander, 780th Military Intelligence Brigade (US)), and Dr. Isaac R. Porsche III (Associate Director, Forces and Logistics Program, RAND Arroyo Center).

The panel opened with General Cardon's reflections on how rapidly the US Army's cyber community and capabilities have grown. Last year the Army had ten cyber teams, this year it has thirty-two, and next year it will have forty-five. The Service has completed the first stage of its network hardening. Branch 17 (Cyber) now has a thousand people. And the Army Cyber Institute has been founded to "look over the hill" at the future of cyber. Cyberspace has had a pervasive impact on every aspect of the military. Cyber effects can be both extremely destructive and extremely enhancing. All cyber operations are converging in a way they had never done, even as recently as a year ago.

Singer noted the way interest in the field is growing, and tossed out some rough figures to characterize that growth. "I'm struck by the title of this panel: cybersecurity is a field shaped by amazing trends. When today's twenty-year-old soldier was born, there were fewer than twenty thousand websites. Now there are three billion." The threat has increased dramatically over that time as well. To take just one indicator, the number of identified viruses then stood at ten thousand. Last year alone three hundred seventeen million new pieces of malware were developed. "At least a hundred nations have a military-level capability in this regard." The Department of Defense budget mentions "cyber" over a hundred times. Antimalware and antivirus companies are realizing one hundred sixty billion in revenue.

We can expect to see thirty billion new devices come online over the next ten years, will some trillion sensors collecting information on us. "This growth will be concentrated in areas of the world where conflict is most likely. 70% of mobile users are in developing areas of the world. More people in sub-Saharan Africa will have cell coverage than electricity. So, Singer asked the panel, "How do we win in a complex world?"

Old Ideas Turned Over in New Ways

Porsche took the floor first, offering observations in the spirit of Mark Twain (who, Porsche noticed, was an inventor as well as a writer). We keep turning to old ideas in new ways. We find ourselves defining and redefining information operations over time. There are new thoughts and ways of doing things that we haven't thought of yet. Information and cyber operations have been studied for two decades, and we have a lot of good thought to choose from.

"Issues in cyberspace," he argued, "can be boiled down to people and tech. The challenges and opportunities come from these two categories." He noted that at one time there was no

punishment for infractions like taking home laptops from a SCIF. “Now that’s unthinkable,” he said, optimistically. (We must observe in the interest of historical truth that there have long been punishments for casually mishandling classified information. If there were once no punishments for carrying a secure laptop home, that’s largely because laptops had at that time yet to be fielded.)

But, Porsche went on to say, “What has not been addressed is the overlap that exists between network operations, cyber operations, and other areas of the Army.” These ought properly to be regarded as a “unified whole.” Interoperability is the key to collaboration, and collocating personnel who share a common vocabulary enhances interoperability. The lowest level of interoperability is what he called “swivel chair interop,” sharing information about missions.

He that connectivity and interoperability have both physical and semantic levels. The latter is often more difficult to achieve than the former. Porsche point to the Afghan Mission Network, created to allow coalition partners to share information, as an example of successful interoperability. “They figured out how to get around interoperability issues. They created translators that helped all systems talk the same way. All stakeholders got together to develop this, and it took continuous effort by a large number of people to make this happen. Learning by doing, it took years. We no longer have the luxury of that amount of time.”

The size of cyber devices is shrinking, as is the cost of entry into the market. We will have more data to exploit, but so will our enemies, and we will race to make the most innovative use of the data that are out there. “Current trends are driving us to innovation. Devices are being put in people’s hands, and the Army needs to change faster to overcome outdated red tape. What the Army needs to do for cyber is put the groups together who work best in cyber, and have the same thought processes.”

The View from the (Metaphorical) Factory Floor

General Fogarty spoke next. “I’m in charge of basically a huge factory that works in cyber,” he said, and that drives the capability requirements that will determine what cyber will look like in the future. “To win in a complex world, we must let the Army work in multiple domains. The army works in cyberspace in the same way it works in other maneuver forms.”

The threat has also changed. Some of our adversaries don’t have sophisticated capabilities, but others certainly do. He invited the audience to consider the way the American military fights. It’s dependent, he said, on command, telemedicine, cyber, etc., and on many other things we can’t deploy without. “We need to understand the importance of the network. The greatest threat I face is not enemy tanks, but enemy cyber. How we try to defend ourselves in cyber will determine how well we can fight. Our enemies have had fourteen years to observe us and see how dependent we are upon cyber abilities to act.” The challenge we face is assuring our access to critical networks while simultaneously denying that access to our adversaries. To do so we need to “ present our enemies with multiple dilemmas.” Our critical capability gaps include a unified cyber platform and coordinated attack capabilities.

Fielding and Leading the Cyber Mission Force

The US Army has made “tremendous progress” building out the Cyber Mission Force, Colonel Hartman said. We have national mission teams, a National Guard unit at Fort Meade, and the complete build-out of three additional teams (including detachments in Texas and Hawaii).

He pointed toward progress in collective training programs. Two installations now have physical space for a team and an opposing force, with access to a simulated Internet. “This give us the ability to increase the complexity for the trainees. Our goal is to be able to tell a combatant commander that we can do XYZ because we’ve trained to it so often in simulation.”

Hartman called attention to the hoary myth that the Services do not easily work together. They absolutely do, he said, in cyber: "We all talk the same language." His organization routinely trains with sister Services at Fort Meade, and all their exercises include all the Services as some level. He also described training exercises with combat units at Forts Bragg and Hood. They've learned many useful lessons from these exercises—for example, learning how to locate enemies through social media. Such exercises help deploy a capability that rapidly integrates with a commander's plans.

The Cyber National Mission Force: Operational Convergence

General Nakasone, bringing the perspective of "someone who's maneuvered people within cyberspace," thought "convergence" the perfect topic for the day's discussion. Secretary Carter has been a tremendous supporter of cyber, and the Department of Defense is making a huge investment in the field. We're developing both doctrine and strategies, and we're building, in effect, a cyber maneuver team able to operate in adversaries' networks.

He characterized that maneuver force as "a young force of Millennials," 80% military, 20% civilian, with significant capability in both human and computer languages. Anyone who joins the team can expect to receive between ten to twenty-seven months of very intensive training.

"The adversaries," he stressed, echoing a familiar theme, "understand the idea of cheap, fast, and easy." There's a lot of purchasing of off-the-shelf capabilities, and we're seeing effective use of phishing and spearphishing. "So we're on the wrong side of the cost curve—we're still in the slow, expensive, hard way of doing things."

The adversaries are targeting very sensitive information, as we saw in the Sony hack. They're also working to get into networks to deploy malware that destroys data, and this is particularly dismaying considered as a risk to critical infrastructure.

The private sector's growth is influencing the global infrastructure. Most of the Internet, after all, Nakasone pointed out, is privately owned. "With regard to the Army, it truly is all about partnerships."

He concluded with a call to think like our adversaries. "What do cheap, fast, and easy look like for us? This is all commanders' business. They drive convergence, and they play a central role here."

Questions: Disruption, History's Lessons, Combat Systems in the IoT, Personnel, and Graceful Degradation

Disruption involves not only grabbing the new, but also shedding the old. What, a questioner asked, do we need to get rid of over the next five years. Dr. Porsche noted that as much as we might wish to be rid of old equipment in the field, we can't: it will remain with us for quite some time. General Cardon observed that "The last 14 years has created a generation of leaders who are open to huge change and innovation. I can't tell you what's going to go away, but I can tell you it's going to be different. As the army gets smaller you're going to see a greater emphasis on targeted investments. Training will tell us what we need." General Fogarty thought we'd see the shedding of much baggage and complexity. "Every warfighting system has its own stovepiped data stream, and that needs to change." General Nakasone believed we needed to look at how we advance and pay people, and that changes to legacy promotion and pay models were needed. Colonel Hartman noted that today all teams looked alike. "But in the future, maybe the team that has mission X doesn't have to look like all the other teams." The emerging missions aren't here just yet.

To a question about applicable historical parallels, General Fogarty cited the Yom Kippur War. "I think the '73 War was instructive. We had a tangible threat and we drove programs that serve

us today. We saw a fundamental shift in how we trained. General Nakasone thought late 1980s training and the attendant development of common standards to achieve a basic level of competency in all units offered a good lesson for Army cyber. And continuing to move nearer to the present, Colonel Hartman advised a look at the early days of intervention in Afghanistan, where we had a good but imperfect capability. Today we have many high-end capabilities, but they remain to be fully integrated in all forces.

Pointing out that an Abrams tank runs on two million lines of code, a questioner asked the panel to address the cyber threat to our platforms. They are, after all, now a part of the Internet-of-things. With respect to our own military systems, Colonel Hartman thought this pointed out a need to align ourselves with those who are experts in defending IoT systems. General Fogarty noted that "A lot of enemies may not know about all those lines of code or even understand how they work. Commanders have to think about this as never before. Mobile, satellite, SIGINT, the ability to communicate with other commanders is unlimited and we're not teaching this at the level we should. We have to start this conversation early in an officer's career." General Cardon noted the need for building resilience into combat systems. "I think there's a danger in thinking that we can defend all things at all times. The danger is looking at it from our point-of-view and not the attacker's. You saw the 60 Minutes report on hacked cars. The designers did not envision how hackers were going to attack the cars." Dr. Porsche pointed out that vehicle designers have been dealing with onboard networks since the 1970s. He found it significant that the first employment ads for computer defense engineers weren't seen until the late 1990s.

We're using terms like "interoperability." A questioner asked how we were to assess third-party cyber security, the security of our international partners and private contractors. General Nakasone said that our allies have a wide range of abilities, and we should ask what we're going to bring those allies in times of crisis. We look at our networks and decide what has to be protected first. General Cardon reminded the audience that "Private industry sees many of these threats first." We need, he thought, better partnership with industry and better information sharing. "We have twentieth-century laws and policies for twenty-first-century problems."

Pointing out that the total force included the active Army, the Army Reserve, the National Guard, and private contractors, a questioner asked about the future of each in cyberspace. General Cardon said, "We're working hard with the Guard and Reserve on cyber. Many of our members actually work in this area in their civilian life. We need a different construct to take advantage of this. We need to do this much faster." General Fogarty said that all elements of the total forces needed to meet the joint standard. The National Guard training center in Little Rock is effectively training people to standard of excellence in cyber security. "When we talk to generals," Fogarty said, "we tell them they have to make a commitment to [constant updating and training] because experience gets old fast." General Nakasone said, about the National Guard, that "The piece I would add is, how do we help them? There should be a rapid equivalency program. Someone who's worked in Silicon Valley or NSA should allowed to bring that experience to their National Guard service." Dr. Porsche thought "professional hackers" had expertise the Army could use: "They bring in this experience and we need to train them up to military grade."

So, a questioner asked, how much of the Department of Defense's cyber force needed to be in uniform? General Cardon thought there uniformed military ethos was an important one. Combining it with technical expertise strengthened the force.

To a question about training in degraded or lost expertise, like traditional celestial navigation, General Fogarty answered that "We still train people to know how to do things when high-tech things break down. They've gotten a lot better at understanding what the threat to the network is, what parts can be cordoned off in the event of an attack."

It seems, a member of the audience said, that we're not going to get a new cyber Geneva Convention. Are we headed for a no-holds-barred battle in cyberspace? How are we training our commanders on the legal side of this? "There is," General Cardon said, "a number of larger questions here. We shouldn't build a capability that we'll never get the go-ahead to ever use. When we go down the cyber road there are so many questions we haven't answered." Colonel Hartman said that his organization had a cyber lawyer with relevant and necessary experience. "Everything goes through a legal review, and we have a good relationship with the cyber law center in Charlottesville that trains some of the JAGs in this area."

The final question asked the panel what advice they would give a young officer who would be in their shoes one day. We're looking, Colonel Hartman answered, for computer scientists and people with experience, "But we're also looking for true leaders. There are several guys in the audience here who are skilled in computers, and what do a lot of them want to do? Go to Ranger School. They want to be great leaders." General Nakasone's advise was to take a long-term approach. "Entering the Army in the Reagan years was so different from today. When we started Cyber Command five years ago, we had no building, no program, no money. Now, five years later, it's all different. To General Fogarty, "The technical stuff is pretty straightforward—how do you apply it against a particular challenge? Get out of your safe space, accept risk, and you will become a great leader." Dr. Porsche talked about the first military people who began working in cyber. "People in the military who joined cyber before there was a branch, they knew it was going to hurt their careers. It's cool now, but back then they were taking a huge risk. They were dedicated and they stayed in it." General Cardon had the last word. "In my first five years in the Army, it was pretty static. What keeps you going now is cyber. There's a technical component, operational components, and a character component. At the end of the day, it's about people, and how they're going to use these concepts and doctrine to prevail and win."

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 10.20.15