



**CYBER BEACON V**  
Conference Proceedings

September 19-20, 2018

College of Information and Cyberspace

National Defense University

Fort McNair, Washington DC





# National Defense University

## Non-Attribution Policy

All sessions and discussions at Cyber Beacon V were governed by the following NDU Non-Attribution Policy:

(1) So that guests and other University officials may speak candidly, the University offers its assurances that presentations and discussions will be held in strict confidence. This assurance derives from a policy of non-attribution which is morally binding on all who attend.

(2) Specifically, the non-attribution policy provides that:

(a) Without the express permission of the speaker, nothing will be attributed directly or indirectly in the presence of anyone who was not authorized to attend the conference.

(b) Unclassified information gained during lectures, briefings, panels, and discussions may be used freely. However, without consent, neither the speaker nor any element of NDU may be identified as the originator of the information.

(3) This policy of non-attribution will be strictly maintained except when the visiting speakers make public release of their own remarks.

## National Defense University

National Defense University (NDU) was established in 1974, and is comprised of five graduate colleges and several research and support centers. NDU has campuses in both Washington, DC and Norfolk, VA.

NDU's mission is to educate rising national security professionals through rigorous academics, research, and engagements in order to develop critical thinkers and prepare future global security leaders to succeed in strategic assignments.

## College of Information and Cyberspace

The College of Information and Cyberspace (CIC) is one of the five NDU graduate colleges, located at Fort McNair in Washington, DC.

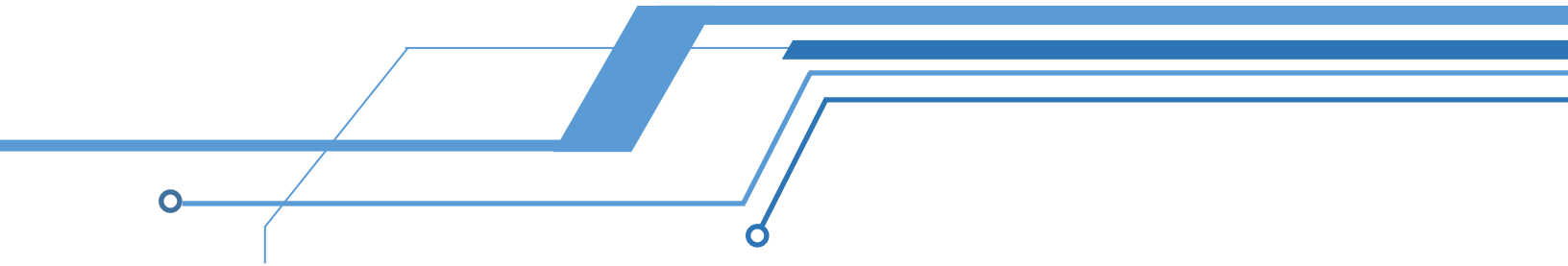
CIC's mission is to prepare its graduates to lead national security institutions and advance global security in the information environment.

## Acknowledgement

Cyber Beacon V was generously sponsored by the NDU Foundation, Circadence, Oracle, Emagine It, and Rockwell Collins.



Conference Proceedings by Jennifer H. Mandula, Cyberspace Education Analyst,  
College of Information and Cyberspace



# Letter from the CIC Acting Chancellor

Colleagues,

Cyber Beacon V was hosted on 19-20 September 2018 by the College of Information and Cyberspace with support from the National Defense University Foundation. The conference hosted over 200 speakers and participants from across DoD, the interagency, the private sector, and academia. Over the course of two days, these participants wrestled with some of the most pressing challenges to national security.

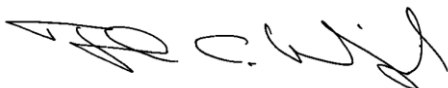
Cyber Beacon V included eight keynote speeches, five panels, and one interactive game-designing session. Perhaps most valuably, attendees engaged with one another, making connections and forging relationships that will push forward efforts in innovation and collaboration.

The theme of the conference this year was Decision-Making in Cyberspace. As we heard many times throughout Cyber Beacon V, the nation is now in persistent contact with adversaries in the cyberspace domain, and is also the focus of multiple foreign disinformation campaigns designed to sow distrust and division.

The College of Information and Cyberspace is working diligently to educate national security professionals to prepare them to respond now and in the future to these threats. We hope you will continue to engage with us throughout the year to discuss and advance ideas—in the classroom and beyond.

We look forward to hosting you again next year for Cyber Beacon VI.

Sincerely,



Thomas C. Wingfield



# Cyber Beacon V Agenda

Wednesday 19 September, 2018

Opening Remarks: VADM Fritz Roegge, BG(Ret) Jack Pellicci (NDU Foundation Chairman), and Tom Wingfield (Acting Chancellor of NDU CIC)

Speaker: GEN Paul Nakasone (CDRUSCYBERCOM and DIRNSA)

## **Session 1: Deterrence**

Speaker: ADM (Ret) Bill Studeman (former CIA Dep Director and DIRNSA)

Panelists: Stephen Peterson (USCYBERCOM Advisor), Dan Johnson (Director of Oracle Strategic Mission Initiatives), Dr. Vaughn Standley (Dept of Energy), and Beau Woods (Cyber Statecraft Initiative, Atlantic Council)

Panel Moderator: COL Nancy Blacker (CJCS Chair at CIC)

## **Session 2: Law/Authorities**

Speaker: RDML Dave Dermanelian (Commander of US Coast Guard Cyber Command)

Panelists: Gary Brown (former USCYBERCOM SJA), Matthew Slowik (DHS Cybersecurity Attorney-Advisor), and LtCol Kurt Sanger (USCYBERCOM Office of the Staff Judge Advocate)

Panel Moderator: Tom Wingfield (Acting Chancellor of NDU CIC)

## **Session 3: Gaming and Cyber Strategy**

Jennifer Mandula (CIC Cyberspace Education Analyst) and Hyong Lee, Center for Applied Strategic Learning (CASL)

# Thursday, 20 September, 2018

Speaker: Jason Healey (Columbia University)

Speaker: MG(Ret) Joe Brendler (former USCYBERCOM Chief of Staff)

## **Session 4: Innovative Collaboration**

Speaker: Col Mike McGinley (DIU Boston Lead)

Panelists: The Honorable Zachary Lemnios (VP of Physical Sciences and Government Programs at IBM), RADM(Ret) Janice Hamby (CIC Chancellor Emerita), Mike Moniz (CEO of Circadence), and Paul de Souza (Founder and Director of the Cyber Security Forum Initiative)

Panel Moderator: Harry Wingo (Cybersecurity Faculty Chair at CIC)

## **Session 5: Information/Disinformation**

Speaker: JD Maddox (Global Engagement Center, State Dept)

Panelists: COL Max Thibodeaux (Joint Information Operations Warfare Center), John Petrik (Editor of The Cyber Wire), Siobhan MacDermott (Global Cyber Public Policy Executive at Bank of America), and Dr. Haroon Ullah (Chief Strategy Officer of the US Agency for Global Media)

Panel Moderator: Jim Churbuck (CIC)

## **Session 6: Cyber Graduate Education**

Speaker: Dr. Pano Yannakogeorgos (first Dean of AF Cyber College)

Panelists: Col(Ret) Jerry Lynes (JS J7 Dep Dir for Joint Ed and Doctrine), LtCol Mark Reith (Dir of the Center for Cyber Research at the Air Force Institute of Technology), Tom Wingfield, and Dr. Cynthia Irvine (first Chair of the Cyber Academic Group at the Naval Postgraduate School)

Panel Moderator: Dr. Cassandra Lewis (Associate Dean for Academic Programs at CIC)



# Deterrence

## Discussion

The US strategy of cyberspace deterrence has thus far successfully prevented cyber acts above the threshold of armed attack, after which the law of armed conflict would apply, but has been unsuccessful at deterring actions that fall below it.

Deterrence is fundamentally about consequence: do adversaries know the consequences of action, and do they fear them? As the discussion noted, the US has been reluctant to declare red lines in the cyberspace domain, which means that cyber-capable adversaries are not aware of 1) the threshold for US response or 2) the available response capabilities. Furthermore, the success of a deterrence strategy relies on a deterrable adversary; when anyone with internet access can pose a hostile threat, it is no longer reasonable to assume that all malicious actors can be deterred. There was therefore some consensus that deterrence models from the past (i.e., nuclear) are not appropriate to discussions of deterrence in cyberspace.

Speakers and panelists noted that while the US frequently defaults to a discussion of cyber vulnerabilities, adversaries have recognized the extraordinary strategic possibilities of cyberspace and they have far more to gain and far less to lose than the US.

## Insights and Ideas

- Defining red lines will require a commitment to attribution and associated identifying technologies
- US adversaries are strategically using cyberspace to sow division and distrust; notably, the Chinese have a word for deterrence that includes the concept of coercion
- US embraces a free and open internet, and has inaccurately assumed that the rest of the world would as well



# Law/Authorities

## Discussion

Law can be a mission enabler rather than a mission obstacle; law provides certainty through boundaries and framework for action. Responding to the deterrence sessions, discussions focused on how the US can engage adversaries who are operating in the poorly-defined gray areas below the threshold of armed conflict. The US can either do nothing, engage similarly by conducting aggressive but not use of force actions, or push for changes in international law.

International norms come about when states agree to current practices, and the same is true of the cyberspace domain. To push international law forward, states will need to publically acknowledge and explain their actions in cyberspace.

Speakers and panelists discussed the specific roles of CYBERCOM, Department of Homeland Security, and US Congress. It was noted that most US government actions in cyberspace going forward will be considered traditional military activities, with significant changes for cyber actions not only in DoD, but throughout the government.

## Insights and Ideas

- Actions below the threshold of armed conflict are not actions the US cannot address, they are actions the US has chosen not to address
- CYBERCOM does not have the authorities to effectively protect certain non-DODIN networks, though it can be argued it has responsibility to do so as part of preparing defense of the nation
- DHS will implement some mandatory measures for private companies
- The majority of Congress's current role in cyberspace involves clarifying existing authorities and prompting the executive branch
- No hardware or software developers have been held accountable for releasing flawed devices and software



# Gaming and Cyber Strategy

## Discussion

Multiple panelists, speakers, and guests at Cyber Beacon V called for expanding the use of gaming and simulation to help prepare today and tomorrow's cyberspace and information workforce and leaders. The interactive design session led by CIC and the Center for Applied Strategic Learning (CASL) at NDU closed out the first day of Cyber Beacon V, with participants working in teams to design and put forth ideas for exactly this type of game.

CIC and CASL intend to use these design suggestions to develop a working wargame that can be deployed across the national security community. Some key trends and themes emerged from the game design submissions, which suggest that these characteristics are sought in cyber and information wargames.

## Insights and Ideas

- Many suggestions for roleplay-style gaming, to include political, industry, military, intelligence, and state and non-state adversaries
- Involve different victory conditions for players based on role or character; possibility for these conditions to be secret
- Practice decision making, value proposition assessment, and risk-reward calculation
- Include an inciting crisis event such as a critical infrastructure attack or foreign influence campaign
- Cooperative and collaborative gaming, with or without an individual winner

# Innovative Collaboration

## Discussion

The modern competition for global economic preeminence is, in many ways, a race to be first to develop the next generation of innovative technologies. This next generation of technologies includes artificial intelligence, quantum computing, and autonomous systems, as well as enabling technologies to advance both technical and human systems.

For the US to win these critical technology races of our time, it must invest and partner with the private sector in developing and advancing innovative technologies. Discussions noted that commercial research and development investment dwarfs that of the combined Defense Industrial Base.

Innovation is intrinsically linked with risk, and the US has historically been reluctant to risk the failures required for forward movement in innovation. Collaboration with private sector can ameliorate this risk, but the US government as a whole must also speed acquisition processes and foster internal innovation.

## Insights and Ideas

- Crowdsourcing may be a way forward for broadening the reach of and speeding innovation
- If DIU (formerly DIUx) is dissolved in several years, it will be a net-positive, signaling that the principles of simple solicitation, negotiation, and accelerated awarding of contracts have been embraced across the DoD
- Private and public collaboration must fully embrace the value of their different perspectives as critical to innovation



# Information/ Disinformation

## Discussion

The US invented mass marketing and modern advertising, and is the center of the film and television industry. And yet, the US has proved surprisingly vulnerable to strategic disinformation campaigns, particularly those of Russia and China. The primary goal of these campaigns is to reduce trust in US institutions, such as government and media, and attendant principles, such as democracy and capitalism. Notably, Russia and China are even more invested in disrupting information and sowing disinformation in emerging democracies, which will likely have long-term ramifications for the global environment.

Investment in AI technology for identifying and predicting disinformation campaign may be able to slow or impede the spread of disinformation. However, the problem is fundamentally one of human behavior: people believe things that align with their existing belief frameworks. Countering malicious disinformation, therefore, requires a large-scale framework that involves media system resilience, fact-checking mechanisms, disinformation detection techniques, and a national narrative and sense of shared purpose. Discussions noted that this last—a shared national narrative—is a particular challenge for the US right now.

## Insights and Ideas

- Geopolitical borders are no longer the defining characteristic of community; common language has assumed that role, making “lexical” rather than national communities
- Emerging research suggests that states with significant investment in public media are more resilient to foreign interference
- There is no US governmental actor looking for broad trends in disinformation campaigns; resources are currently only focused on removing bad-actors

# Cyber Graduate Education

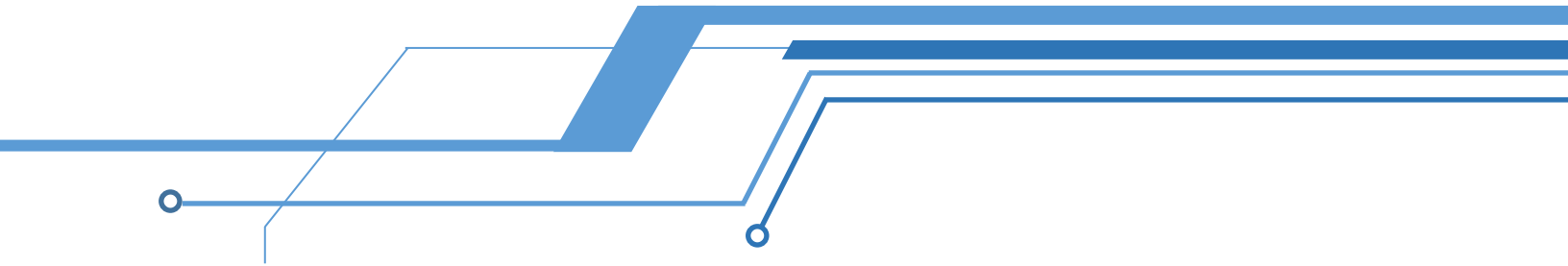
## Discussion

DoD cyber education at the graduate level has the challenge of balancing both immediate needs and skills with preparation for future, long-term needs and skills. This is particularly significant given the fast rate of change in the cyberspace domain. Students need to be educated not only on current technologies and cases, but on broad frameworks and theory that can be applied to future technologies and incidents. Nevertheless, DoD cyber education must be able to adapt at a faster rate of change to integrate current technologies into curriculum.

Government, military, industry, and academia are competing for the same limited cyber workforce and experts. It is therefore imperative that cyber education be integrated earlier and more fully into DoD training and education at all levels.

## Insights and Ideas

- Leveraging experiential and active learning in cyber graduation
- If there are to be significant changes to JPME education, the JPME granting institutions themselves will need to lead the push to revise the OPMEP
- Digital natives are not an 'automatic' cyberspace workforce simply because they have grown up with computers; we will continue to require a cyberspace education ecosystem



Save the Date:  
**CYBER BEACON VI**  
11-12 September, 2019