INTELLIGENCE OPERATIONS IN A DIGITAL AGE

PANEL HIGHLIGHTS

On June 24, 2019, the Council on Intelligence Issues (CII) sponsored a panel discussion of experts on the topic "Intelligence Operations in a Digital Age." The panel was part of CII's efforts to educate the public about the practical, policy, and legal factors that influence the planning and conduct of clandestine intelligence operations, how technological advances can affect operations in an increasingly transparent world, and the challenges and risks that confront intelligence officers, their agents, and others who assist them to support U.S. national security objectives. This article presents highlights rather than a summary of the evening's discussions.

The panel consisted of former government officials: CIA head of the national clandestine service Michael Sulick, NSA official Daniel Ennis, DNI chief counsel Robert Litt, CIA chief counsel John Rizzo, DHS Undersecretary Suzanne Spaulding, and CIA information operations chief Kevin Zerrusen. See more information about the panelists at the end of these highlights.

In opening remarks, one panelist captured the challenge posed by technology and the digital age: "Cyber changes everything. Everywhere today, everything is out there, and there are lots of opportunities for getting it." Denying access, whether by U.S. or foreign intelligence, is almost impossible. "If you can imagine it, you can do it." A big challenge is speed. This leads, in some ways, to the result that past ways of doing business, and responsibility for who does it, will not work today.

"Key takeaways" from the panelists included:

- Cyber has fundamentally changed how we think about intelligence and how we conduct intelligence operations.
- The half-life of secrets continues to shrink, and we need to rethink how we have operated in the past.
- We need to challenge ourselves in getting information to the public. We have to assume it will come out, so think about how we gain or lose our advantage as an open nation if we do or do not classify information.
- Title 10 and Title 50 distinctions between how the military and the IC conduct as either traditional military operations or covert action is worth a look, but cyber is only one piece of a much larger context.
- Legal and policy reviews and congressional oversight of operations are important. In any investigation of a controversy after an operation or failure, the people who really are

affected are not those who approved operations, but the career analysts and operators who carried them out. They may need to hire lawyers.

- Whatever technology challenges may exist, an effective intelligence capability still must include HUMINT operations that can adapt, and has been adapting, to the challenges.

In opening remarks, one panelist captured the challenge posed by technology and the digital age: "Cyber changes everything. Everywhere today, everything is out there, and there are lots of opportunities for getting it." Denying access, whether by U.S. or foreign intelligence, is almost impossible. "If you can imagine it, you can do it." A big challenge is speed. This leads, in some ways, to the result that past ways of doing business, and responsibility for who does it, will not work today.

Law and Policy:
Panelists highlighted the basic rules that are considered and general approach in planning offensive cyber operations: Is there U.S. authority, which agency should conduct it, whether the action is the use of force under international law, with this latter point somewhat complicated and difficult to resolve. Also considered are foreign sovereignty issues, domestic law prohibitions including the notion (remarkable to many attendees) that there is a First Amendment right not only to speak but to "listen" to the views of others. One panelist pointed out the challenge in conducting operations in accordance with often ambiguous legal requirements: "There's a disconnect between what we don't want people to do to us and what we do want to do to them."

Covert Action vs. Traditional Military Activity Lines Blur:
More than one panelist noted that there is a large "loophole" as to what is and is not considered "covert action" that requires specific presidential prior approval. The recent legislation actions that label cyber military operations as "traditional military activities" seemingly has opened the door to a broader range of activity being conducted without the longstanding executive branch review and congressional oversight. On the other hand, one panelist noted that the need for speed because of the risk of losing technological or other advantage is part of the reason for changes to the more traditional Title !0 and Title 50 approaches.

Importance of Oversight:
This divergence between Title 10 military operations and Title 50 intelligence operations is of particular importance for another reason. One panelist noted the risks this can pose for intelligence officers who carry out lawful orders but are then investigated to determine "accountability" when the operations have unintended consequences. These could include loss of life as well as property and potential retaliation against U.S. industry. In the past, it's tended to be the officers told to engage in operations who are investigated, but less so for the more senior persons approving the operations.

It's Not Just Cyber:
Another panelist stressed the need to look not only at "cyber" solutions but all possible solutions to threats. The DNI has a mandate to look broadly at all possible options, not just cyber responses. The Cyber Threat Integration Center provides another mechanism for a whole of government approach. The panel agreed that a strategic look is needed, not just case by case reactions.

It's Not Impossible:
One panelist commenting on non-cyber option, HUMINT operations, highlighted the difficulty of operating in a digital world. Street cameras, facial recognition, digital scanning of documentation, and the speed at which adversaries can use technology to identify undercover officers all pose challenges to operators. A panelist asked, "Is it impossible to have a false identity or operate in alias?" Answering his own question, he stated, "No, but this is cumbersome. It's difficult, but can be done."

Shelf Life of Secrets is Shrinking:
Another challenge is that "the shelf life of secrets is vanishingly short." Technology has made it so much more difficult to keep secrets, so that in 2010 one intelligence official said that "in 10 years there will be no more secrets." This led one panelist to urge that the importance of using one of America's great vulnerabilities, openness, as a strength in dealing with our more restrictive and authoritarian adversaries. We need to "train to fight in the light" as this plays to an American strength. Adapting to a more transparent world will best ensure protection of national security.

Public-Private Sector Collaboration Is Essential:
Adapting to the challenges will take collaboration with the private sector, perhaps not all at once but by sector, such as financial sector, or critical infrastructure elements, more than one panelist suggested. Russian attacks on the U.S. legal system and the courts, Russian disinformation and propaganda including little known efforts to undermine FISA, raised the question of what role the intelligence community should play in educating the U.S. public, including elements of the private sector whose economic, privacy, and other interests are under attack.

Threats to Private Economic Interests:
The risk to private interests highlights another reason to engage with the private sector to determine possible solutions to address foreign cyber operations. One ongoing effort cited was

the Financial Systemic Analysis and Risk Center, which is designed for the private sector to work with the White House by receiving classified information and coming up with solutions.

Educating the Public -- Facts Over Guesswork:
Panelists tended to agree there is an important IC role, but that role should focus more on getting the facts out, not on propagandizing the public. The media and private institutions should play a more constructive role in presenting facts and identifying misinformation. One panelist noted that never before have more intelligence officers been on T.V. This has had both positive and negative consequences as some have been seen as too political, which in turn raises questions about the objectivity of the IC. When asked if intelligence officers should be so visible, one panelist responded that "I don't want to see more *retired* officers. We must have people who are engaging in real [public] dialogue, not guessing."

Draw Upon America's Strength -- Greater Transparency:
The massive public disclosures of information from cyber intrusions and theft have actually led to an increasing willingness of the IC to discuss its work more freely, and to reach out to some in the press to provide a better understanding to the media and the public. At least one media representative in attendance agreed and expressed the benefits this brings. Enabling intelligence agencies to share more with the private sector, to declassify even information historically denied to protect sources and methods, will be increasingly important. To date, this has been somewhat episodic, with a panelist observing that the IC has seemed to be less proactive in pushing information out where there have not already been public disclosures forcing the IC to react. More public releases by the IC are needed to inform and educate, but not so as to influence the public surreptitiously. An important goal is to restore public trust by highlighting the threats, not grading the media or to politicize.

General -- Attendees Added Value to the Discussions:
At the outset of the discussions, panelists encouraged the attendees to ask questions at any time and not wait until the end. Accordingly, questioning from the more than 100 attendees was robust with extensive follow up and interaction. Topics such as the impact on competitiveness, supply chain challenges, the impact of disinformation and propaganda, and the relative inability of the U.S. to formulate coherent and comprehensive responses triggering strong views from attendees who thought the U.S. should be doing more to educate about the threats. One panelist pointed out that the IC collects intelligence to use it, and that "maybe the consumer is now the public."

When asked what mechanisms panelists might suggest by which there could be meaningful change, panelists tended to agree that legislation and mechanisms – reorganizations or a new

agency -- won't be as effective as cultural changes. One attendee noted that most in attendance shared "the same view that we are struggling at best to deal with the threat, especially with a White House and bipartisan oversight committees that are unwilling and/or unable to support the Community's efforts." A panelist said that DHS is the one department that could lead a "whole of nation" approach.

Thanks to Event Co-Host: The panel ended with CII co-founders Bill Murray and George Jameson thanking event co-host Steptoe & Johnson for its support, encouraging attendees to offer suggestions for future events as well as to volunteer legal and other counseling to support intelligence officers needing assistance.

Fall Event Being Planned: CII also announced that it is planning to gather a panel of former intelligence officers to address analytic and operational objectivity. This will highlight the challenges of speaking truth to power, bringing bad news, avoiding politicization, and related matters. The event will be held in the Fall in collaboration with the International Spy Museum.

MORE ABOUT THE PANELISTS

Michael Sulick, Moderator

- Consultant, Insider Threat Issues and National Security Affairs
- Former Director, National Clandestine Service, CIA

Daniel Ennis

- Executive Director, Univ. of Maryland Cyber Initiative; CEO, DRE Consulting
- Former Director, Threat Operations Center, NSA

Robert Litt

- Of Counsel, Global Risk & Crisis Management, Morrison & Foerster LLP
- Former General Counsel, Office of the Director of National Intelligence

John Rizzo

- Consultant, Steptoe & Johnson LLP
- Former Deputy and Acting General Counsel, CIA

Suzanne Spaulding

- Senior Adviser, Homeland Security, International Security Program, Center for Strategic and International Studies
- Former Under Secretary, National Protection & Programs Directorate, DHS

Kevin Zerrusen

- Managing Director, Goldman Sachs
- Former Director, Information Operations Center, CIA