

# Intelligence, National Security, and War – Cyber Panel

---

Dick Crowell  
Naval War College

The cyber panel brought together experts from the corporate, academic, and military communities to discuss the accelerated intertwining of cyberspace and human activity to better understand their relationships with respect to intelligence, national security, and war. What follows is a summary of the panelist discussion combined with comments and questions designed to promote thought on how cyberspace affects these important aspects of national security.

**Jim Cowie**, co-founder and chief technology officer for Renesys, the Internet Intelligence Authority, opened with a brief description of his company and the services they provide. Renesys studies, maps, and measures internet connectivity. By monitoring over 500 internet service providers (ISPs) along with more than 100 infrastructure nodes they are able to take in excess of a billion measurements a day in the study of the evolving internet connectivity. The knowledge gained on routes to connectivity has a commercial value to the corporate world and others.

Jim stressed that the internet was not built for governments or militaries. However, we must understand the terrain and understanding the internet is a large part of the cyberspace. He presented the concept that countries have spheres of influence on the internet just as they have in the physical spaces. He likened this to the ‘Great Game’ that played out in the nineteenth and twentieth centuries between European powers. Jim’s thesis can be seen playing out in the Caucasus and across Europe as countries want to be free from the political and economic influence of current or former great powers.

Countries with previously created dependence on commodities such as natural gas, oil, and communications now want to be free from their ‘protectors’. In the Republic of

Georgia, the scene of the 2008 Russia-Georgia war, itself a vestige of the Great Game, the people want to move away from the Russian communication networks toward their own. Their previously heavy reliance on Russian communication infrastructure and connectivity can be seen as a political and military vulnerability in that war. In the middle of the war a long haul submarine cable was laid across the Black Sea from Varna, Bulgaria to Poti, Georgia. While not available for use during the conflict, this fiber optic cable now brings high speed connectivity to Georgia and frees them from dependence on both Russian communication networks and costly services through neighboring nations.

Additionally Jim brought up the importance of understanding firm attribution and identity on the internet. He stressed the risk to political and military decision makers relying too literally on the ability to identify those who break laws and use the internet for illicit purposes. He described the vignette where *Pirate Bay*, a website that provides an index to the global pool of BitTorrent content (a practice of peer to peer file sharing that is used to share large amounts of data over the internet, often related to illegally selling music and video files), announced they had moved their servers to a data center in Pyongyang, North Korea. Many highly respected Internet analysts believed it to be true, but in reality it was a failed attempt at an elaborate deception operation meant to avoid European law enforcement. Jim cautioned that understanding this type of deception may be useful to future national security.

**Ryan Maness** from the University of Illinois at Chicago brought the Cyber Espionage question to the panel. Ryan has co-authored with Brandon Valeriano a chapter on the theory of cyber espionage for an upcoming book. Ryan brought out that while states have used espionage for hundreds of years, what we are seeing in the cyber domain from potential future adversaries supports general theories of rivalry between states. Additionally, the ease of cyber espionage supports use by non-state actors.

Ryan presented three hypotheses to the workshop that centered on using cyber espionage to create rivalries in the physical spaces. These forms of competition will attempt to level uneven playing fields, use international constraints and norms to manage

competition, and place economic costs on rivals. The underlying question centers on understanding what is being done with the vast amount of information that is stolen, often by cyberspace operations, and how it will affect future national security.

Ryan accepts that espionage is one of the oldest professions. He states that historically little damage has been done and espionage is often the outcome is more nuisance than damage. While this may be true to date, our Department of Defence and defense industrial base must come to understand what is being stolen and how it may affect future conflict. Their near total reliance on electronics that moves information through cyberspace to human and automated decision makers amounts to significant corporate, military, and political vulnerability.

**Stephanie Helm** is a retired U. S. Navy Captain who specialized in information warfare and cryptology. A contractor working for the Naval War College's War Gaming Department, Stephanie brought military expertise to our panel. Stephanie stressed the relationship between the operational commander and good intelligence. She questioned how cyberspace changes the Intel cycle, particularly with respect to time, space, and force. What does cyber Intel mean to commanders? She proposes five focus areas with questions and answers to begin understanding the complexity of cyberspace: the nature of the cyberspace domain, the adversary, the intelligence cycle, organizational constructs, and expertise. Perhaps more importantly, she asked how we as a department of defense along with our various intelligence organizations might be able to use Renesys' understanding of the Internet to our advantage.

As military planners and decision makers we use the cognitive framework of operational art to understand traditional military problems. We have developed problem solving processes that proved successful in solving industrial age military problems. The Joint Operational Planning Process (JOPP), along with our various service processes, is very linear in character. In a search for clarity, they allow us to better understand traditional military problems, i.e., how will the Iraqi Republican Guard be used against coalition forces?

Stephanie reminds us that intelligence is not merely a compendium of information. The information must be analyzed and placed in context in order to become useful intelligence. Where does the analysis begin? Albert Einstein once said, “Nature is kind, if you ask it the right question, it will give you the right answers.” One of the problems with cyber Intel today is that few if any understand what questions to ask. Stephanie goes on to say that great intelligence is predictive and provides deep insight into the adversary’s intentions. Perhaps her most important focus area is human expertise. While cyberspace has greatly changed the character of future war, its most enduring feature, the human has changed little between the industrial and information ages. We need to use the source that invented cyberspace to help understand it and its relevance to future wars, the human mind. It is the human that will eventually ask the right questions to get the right answers. Until then, do we have any idea what is being done with the petabytes of information stolen from civilian and government computers?

## Conclusion

One of the greatest critiques of the 9/11 Panel Investigation was that we failed to imagine that anyone would attack our homeland with commercial airliners. How might a similar failure to imagine attacks on our homeland, ones in and through cyberspace, play out? History shows that future adversaries will not fight us toe to toe. They will most likely use some form of asymmetric or hybrid force; cyberspace is a near perfect domain for that type of attack. Cyberspace operations may be used to steal and adapt weapon systems or to move force in the form of content or code to our shores. The near equal access to cyberspace for states, non-state actors, friends and foe presents us with new challenges and these challenges drive the need for us to understand how cyberspace will affect future conflict.

The cyber panel for Intelligence, National Security, and War provided a snapshot of the variety of national security issues nations’ face in the early twenty-first century. There were valuable discussion between panelists and the audience that moved the groups understanding forward. The intertwining of cyberspace and human activity will continue as

governments, militaries, and corporations drive personnel, employees, and consumers to cyberspace for work, shopping, banking, entertainment, etc. Perhaps the most important lesson is that we all have a lot to learn from one another.