Addressing the Cyber Industry's Knowledge Gap

2016 State of the Field Conference for Cyber Conflict

Hosted by Columbia University School of International and Public Affairs (SIPA) &
Cyber Conflict Studies Association (CCSA)

Jason Healey
Nicki Softness
Karl Grindal

Twenty-five years ago, the public's fear of the unknown within the cyber domain was first encapsulated in the phrase 'electronic Pearl Harbor.' Twenty-five years ago, the population would have likely assumed that these fears would be alleviated as cyber-related uncertainties diminished with time. This has not happened. Today, we still lack even the most basic state-of-the-art questions and assertions about the dynamics of the cyber domain, particularly of cyber-conflict, as well as a concrete expectation of the evolution we expect cyber conflict will take. This lack of cohesive agreement in the field for what is known and what is unknown severely limits the contributions of new academics and practitioners by preventing the field from developing a foundation from which to build.

On June 16-17, 2016, Columbia University's School of International and Public Affairs (SIPA), along with the Cyber Conflict Studies Association (CCSA) took their first steps to combat this significant deficiency, and hosted the first annual conference on the State of the Field in Cyber Conflict. The conference, which took place over two days, melded perspectives and recommendations from a diverse gathering of academics, professionals, and practitioners with the hopes of determining the overall state of research on cyber conflict, and thus better preparing the field to mature.

Conference-wide plenary discussions and individual breakout sessions moderated by experts in their fields, covered interdisciplinary topics in cyber conflict. Prior to each breakout session, PhD and PhD Candidate rapporteurs provided detailed research, outlining overarching research questions that have been highlighted in their respective fields, as well as gaps that demand attention. Attendees then debated the relative certainty and value of what consensus has formed around the core questions, and identified immediate and significant attention. Following the sessions, the rapporteurs shared each group's discussion content as well as their overall findings with the entire conference, which are highlighted below.

International Relations

The International Relations session, moderated by Adam Segal (Council on Foreign Relations), sought to contextualize core issues of cybersecurity within the larger scope of international relations, including theories such as deterrence, restraint, power, and influence. The discussion also highlighted the peculiarities of cybersecurity as it pertains to both state and non-state relationships, and its similarities and differences with currently dominating international norms, particularly those governing operational domains. In this context, the association between cybersecurity and arms control sustained consistent attention. Major questions raised by the group included the implications and potentiality of cyber deterrence, the concept and measurements of cyber power, defensive cyber capabilities, the foreign policy impact of cyber operations, diffusion of power in the cyber realm, promotion of cyber norms, regulation of cyber weapon proliferation, and the influence of bureaucracy in cybersecurity policies.

Tactical & Operational Level Dynamics

The Tactical & Operational Level Dynamics session, moderated by Herb Lin (Stanford University, Hoover Institution), explored the linkages and diffusions between cyber operations and the tactical and strategic components of war, noting the inhibiting effects of most cyber actions. The discussion addressed both the history of these operations, as well as state policies regarding their use within foreign policy. With regard to normative considerations, discussants also debated how legal and ethical issues impact cyber operations, and justifications for and against concern vis-à-vis cascading effects. Comparatively, they also deliberated proper designations of responsibility and procedure for command and control authorities, applied both to acts of operational war as well as to cyber espionage. The conversation concluded with an organizational focus, pertaining to state organization of cyber capabilities, and the resource and manpower limitations for implementing effective cyber campaigns.

Intelligence & Adversaries

The Intelligence & Adversaries session, moderated by Neal Pollard (PwC), aimed to uncover the field’s most prominent and justifiable assertions on intelligence and attribution relating to cybersecurity. The conversation acknowledged certain gaps in the literature, namely a lack of practical determinations for how intelligence-gathering differs in cyberspace, and the overwhelming dominance of Western-centric and introspective policy work. Attribution received significant attention as well, namely the difficulties ensuing from the industry’s accessibility and vulnerability to anonymous attacks. However, discussants did note that attribution becomes more plausible when matched with a comprehensive history of cyber-attack patterns, further highlighting the need to establish industry norms and expectations. Takeaways from the session focused on inherent defensive vulnerabilities as well as the near impossible task of determining attack motivation, particularly when the attacker is anonymous.

Strategic Dynamics of Cyber Conflict

The Strategic Dynamics of Cyber Conflict session, moderated by James Mulvenon (Defense Group Inc.), focused its conversation on the established and unknown characteristics of cyber power, deterrence and compellence, attribution, individual and multiple actors, escalation and norms, state sovereignty and international cooperation. Attendees worked to identify existing definitions, and to propose superior terminology for the state of the art information for the cyber field, relating proposals to similar concepts in other domains, and ascertaining the greater normative and dynamic structures governing these terms. In terms of goals and foreign policy planning, the session ended with deliberations on the possible futures of cyber arms control and Internet governance, and for the role of national sovereignty in cyberspace.

Cyber Conflict History

The Cyber Conflict History session, moderated by Jason Healey (Columbia University, School of International and Public Affairs), took a deep dive into the origins of the domain, foundational research in the field, and the contemporary histories reflecting on the implications this history has to the normative and operational dynamics discussed by the other sessions. Initial research and the subsequent discussion sought to connect contemporary history with the earlier history of cryptography, early computing, electronic warfare, and information assurance. Further efforts sought to group cyber conflict history into separate eras identifying key transition points and unique technical and political attributes of those eras, and their effects on governmental and non-governmental institutions. The discussants noted that a lack of comprehensive case studies and an over-zealous focus towards contemporary examples has made it difficult to draw unbiased conclusions or identify historical trends.

Legal Issues

The Legal Issues session, moderated by Harvey Rishikof (Crowell & Moring), attempted to analyze a spectrum of cyber conflict, ranging from permissiveness of non-state actors, to targeted cyber disruption, and total war. Attendees debated the relevance and of both Tallinn 1.0 and Tallinn 2.0 in debating cybersecurity law and ethics, particularly when tasked with understanding and analyzing cyber incidents within international law, governance and norms, cyber-crime and espionage, and cyber-terrorism and sabotage. Gaps identified in the literature included an incomplete understanding of adversarial non-Western, views on international law in cyberspace, and the inability to legally account for certain exceptions. As in the strategic dynamics session, discussants worked to legally identify the constitution of cyber threats and cyber weapons, as well as define cyber infrastructure and states' responsibilities to protect them. The concept of proportionality received significant attention, relating to both threat response and mitigation, and to comparative proportionalities within other domains. Cyberspace was also very generally placed within the legal limitations of other global declarations, such as the Geneva Convention, in efforts to determine how the space differs.