

Toward a Cyberconflict Studies Research Agenda

In January 2003, the Massachusetts Institute of Technology hosted a workshop attended by dynamic mix of computer security professionals, political scientists, economists, engineers, policy wonks, and a few notable government officials (including then-“cyber czar” Richard Clarke).

two different camps, with one sub-canon focused on technical issues with little concern for strategic issues and vice versa.

Research vectors

We can divide the potential research vectors for cyberconflict studies into five large-issue categories: international and national security, legal and ethical, military and operational, new security agendas, and methodological issues. I’ve presented them here in the form of questions to provoke debate and discussion rather than to present finished analysis. Where appropriate, I’ve identified an initial slate of corresponding technical study areas, although many more could and should be added to these lists.

International and national security issues

By definition, cyberspace is transnational, thus cyberconflict in this area raises several thorny problems related to sovereignty in the international realm. Moreover, because of the potentially strategic impact of an attack, cyberconflict must be treated as a subset of the larger literature about strategy honed during the Cold War. Many of the same fundamental questions raised in the debate over the role of nuclear weapons, for instance, are relevant to cyberconflict, although with new and interesting features.

One set of these sorts of questions addresses first-order concerns about assessing the actual potential impact of cyberattacks, particularly because there is no hard “science” of effects like nuclear weapons: Will cyberwarfare constitute a significant form of coercive power? How vulnerable

JAMES
MULVENON
*Defense
Group Inc.*

The main topic of discussion was the purpose and scope of a new cross-disciplinary community—the Cyber Conflict Studies Association—which its founders hoped would provide the basis for a professional field of inquiry on cyberconflict. Although the participants hotly debated the analogy’s appropriateness, most agreed that they wanted to build something similar to the academic and policy field of nuclear conflict studies that developed during the Cold War.

In the two years since the initial meeting, the community has held numerous research symposia on critical cyberconflict topics, but the field still needs to advance focused and policy-relevant research on the strategic and technical aspects of cyberconflict. This article represents a first cut at a cyberconflict research agenda.

Terms

The first step is to define terms, particularly hard-to-define terms like cyberconflict, which many different people have used to describe widely dissimilar phenomena.

For the purposes of this article, *cyberconflict* is the conduct of large-scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks, and infrastruc-

tures, including the use of cyber-based weapons or tools by non-state/transnational actors in conjunction with other forces for political ends. Yet the first task of a cyberconflict studies research agenda is to refine the definition of cyberconflict itself, in particular the difficult task of categorizing formal cyber-based activity between countries (that is, cyberwarfare) vis-à-vis intelligence collection, covert action, crime, terrorism, and war. We also have to consider the “soft” side of information-gathering operations, such as perception management (actions to convey or deny selected information, and indicators to influence emotions, motives, and objective reasoning), deception (measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce a reaction), and other psychological operations (activities to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals). Another important, but no less difficult, categorization problem involves distinguishing between technology research and strategic studies. The current literature is largely divided into

are nations, their critical infrastructures, and key organizations to cyberwarfare? What large-scale effects can cyberattacks achieve? How easily can we protect ourselves from them? Could someone use cyberwarfare to conduct economic coercion such as sanctions, blockades, and so on? Technical study areas to answer these questions should focus on capabilities metrics, defense metrics or indicators of attack, battle-damage assessment methodologies, security relationships across system boundary lines, understanding cascade failures, the economics of cyberattacks, and understanding the interdependencies between business and public sectors.

A second set of questions addresses the fundamental concepts of strategy, including deterrence, credibility, crisis management, and similar core concepts explored during the Cold War in the works of Thomas Schelling and others: Can we use cyberwarfare for deterrent purposes? What factors will govern the capacity of a state or organization to deter a cyberattack? What characteristics of cyberwarfare capabilities will constitute the most effective deterrent against certain types of adversaries? What thresholds for response can we establish? How will adversaries signal intent or communicate during cyberwarfare? How could coercive and deterrent uses of cyberwarfare forces likely fail or fall short? How would cyberwarfare impact crisis stability and crisis management considerations? Will threats of decapitation or paralyzing communications substantially change crisis dynamics, and if so, in what types of situations? What types of events will exacerbate crises involving cyberwarfare? How do difficulties of attribution and spoofing influence these considerations relative to cyberwarfare? What are the possibilities for collateral damage—the unintended effects—from using certain cyberwarfare capabilities? What international systems (such as telecommu-

nications or finance) are most vulnerable to this possibility? How should command and control arrangements be orchestrated? What considerations will impact release authority? How would cyberwar influence war termination dynamics? These issues raise several difficult technical problems, including the attribution of an attack, calculation of attack effects, and battle damage assessment.

A third set of questions involves defensive responses to the threat of attack: How can states and organizations establish the most effective defenses? How will a cyberdefense's effectiveness interact with the effectiveness of other coercive means, particularly economic or military? How will establishing a cyberwarfare defense affect privacy and civil liberties? The corresponding technical study areas must address deception methodologies (both against attackers and BDA efforts); defense metrics, sensors, actuators, and tactics; building trustworthy systems from untrustworthy parts; and the monoculture problem (could multiple operating systems help?).

A final group of questions examines how cyberconflict affects relations among states, particularly the possibility that cyberweapons might allow smaller states to conduct asymmetric attacks against large states: How will cyberwarfare influence regional security dynamics? How will disadvantaged groups or states view opportunities and risks? How will a

ing to the environment and solving problems with respect to the threat or use of force—influence its adoption and use? What are likely conflict approaches or campaign strategies for actors considering the use of cyberwarfare capabilities? Will we see massive strikes on civilian infrastructures or efforts to impact military forces? Are protracted guerilla campaigns likely? How will cyberwarfare capabilities proliferate? What factors could constrain this proliferation? One important technical study topic in this area must be the interdependencies among states sharing an international cyberinfrastructure.

Legal and ethical issues

As a new realm of warfare, encompassing fast-moving new technologies in the hands of both states and non-state actors, the legal and ethical issues involved in cyberconflict are largely *terra incognita*.

One important set of issues relates to the legal definitions of cyberconflict and the implications of conflict in cyberspace for traditional political, social, and economic systems: When does a cyberwar constitute a use of armed force or an actual act of war? What actions would constitute a war crime? Will cyberwar, especially establishing defensive capabilities, have an impact on government–private sector or civil–military relations? Under what circumstances could cyberwar reduce the human, economic or environmental conse-

By definition, cyberspace is transnational, thus cyberconflict in this area raises several thorny problems related to sovereignty in the international realm.

country's strategic culture—its traditions, values, attitudes, patterns of behavior, habits, symbols, achievements, and particular ways of adapt-

quences of conflict? When might it exacerbate consequences?

A second group of questions focuses on the possible contributions of

international, regional, and bilateral treaties in governing conflict in cyberspace: What are the possibilities for international cooperation and

achieve coercive, deterrent, and defensive objectives with cyberwarfare capabilities? How can cyberwarfare capabilities be integrated with other

The field of cyberconflict must sample from a wide variety of methodologies and tools.

arms control in the cyberspace realm? What cyberconflict capabilities or activities might be usefully constrained by treaty or agreement? What factors influence the utility of global, multi-lateral, and bilateral arrangements? Do pledges to not use first-strike cyberweapons make sense, and if so, in what context? What considerations should govern declaratory policy for different actors? How can we establish trust, verification, and enforcement mechanisms?

Military and operational issues

Although cyberconflict is often discussed in the media in the context of hacker attacks against Internet Web sites and the like, many militaries around the world devote considerable resources to exploring the use of cyber-based weapons in military conflicts with state and non-state actors.

The first set of issues deals with measuring and evaluating cyberwarfare capabilities: How can we measure capability? What is the influence of cultural or organizational factors influence these measurements? How can we evaluate conflict scenarios involving cyberwarfare? What are the relative strengths and weaknesses of modeling, simulation, gaming, and exercises? How will cyberwarfare capabilities factor into evaluating conflicts involving other forces? Technical studies must develop metrics for capability that are measurable, even from a distance.

A second group of questions involves military operational issues about cyberconflict: what kinds of targeting strategies would best

military forces? How will they affect evolving operational concepts? How do they influence the development of advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) or space capabilities? How can leaders and personnel for conducting cyberwarfare be trained, educated, and grown? Technical studies should focus on econometric modeling or operations research positing different capabilities against different objectives.

A final set of topics addresses dilemmas posed by military cyberdefense: How can capabilities to enhance transparency related to cyberwarfare capabilities and operations be developed? How can actors more quickly attribute the sources of attacks or disruptions? Will international cooperation play a key role? The main focus of a technical study in this area should be the problem of attributing an attack to a particular attacker, given cyberspace's ambiguities.

New security agendas

Cyber conflict has proven particularly attractive to non-state or transnational actors across the entire political spectrum.

A first set of questions in this area explores the motivations and methods of new cyberconflict actors: How will the variety of trans-state actors (jihadists, anarchists, political activists, criminal organizations, and so on) differ in their approaches to cyberwar? Could cyberwarfare provide impetus or significance to the emergence of new forms of conflict or protest? What would be the con-

straints? Are particular defensive approaches better suited to combating different emerging threats than others? What challenges do terrorist groups and other transnational actors face in establishing offensive and defensive cyberwarfare capabilities? What relative advantages and disadvantages do non-state actors have in developing, using, and controlling such capabilities?

A second group of topics focuses on the implications of the rise of these new cyberconflict actors for traditional states: What would be the impact of vigilantes, hacktivists, and sympathetic hackers on crisis management and war termination? Would they affect the ability of state and non-state actors to mobilize significant capability to conduct cyberwarfare? How might cyberwarfare influence approaches to peacekeeping and peacemaking? Could the possibility for cyberwarfare increase the potential for failed states? How might cyberwar interact with new technologies that could influence conflicts (for example, biological engineering, nanotechnology, and so on)?

Methodological development

To answer many of the questions I've outlined here, the field of cyberconflict must sample from a wide variety of methodologies and tools, ranging from the traditional to the bleeding-edge. Among the key questions that must be answered in this quest, how can we employ traditional approaches (case studies, game theory, quantitative methods, and so on)? What new approaches can we apply? How can we accumulate useful data sets and evidence for research? What types of interdisciplinary teams or approaches seem most fruitful? How can we foster them? How could an interdisciplinary approach shed light on the likely technical, operational, economic, and social impact of a cyber-attack on, say, passenger transportation systems or financial

institutions? How can we apply complexity and adaptive systems theory, theories of failure modes, or theories regarding institutional management challenges of complex systems? How do we apply the concepts of network organizations? How can we improve the means to visualize cyberspace and cyberwarfare? Technical studies must focus on the implementation of these new methods and tools in hardware and software environments.

Whether you're a skeptic or a fanatic about cyber conflict—of even if you fall somewhere in the sane middle ground—there's no doubt that the information revolution and our connected global information infrastructure will play an increasingly important role in strategic conflict. Information technologists, policy experts, and strategists must therefore aggressively systematize our understanding of the possible natures of cyber conflict and its potential implications for our economy, society, political system, intelligence apparatus, and military.

This article is a tentative road map for what will be a long process of developing a cyberwar research field with stable theories and rich case studies, but a journey of 10,000 miles begins with a single step, and this is that step. □

James Mulvenon is deputy director for advanced studies and analysis in the Defense Group Inc.'s Center for Intelligence Research and Analysis. His current research focuses on Chinese command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), defense research/development/acquisition organizations and policy, strategic weapons doctrines (computer network attack and nuclear warfare), patriotic hackers, and the military and civilian implications of the information revolution in China. Mulvenon has a PhD in political science from the University of California, Los Angeles. He is a board member of the Cyber Conflict Studies Association and a term member of the Council on Foreign Relations. Contact him at mulvenon@cira-dc.com.