Atlantic Council
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Chris Demchak

Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered World

A spate of attacks from both state and nonstate actors have provoked other Western nations to join the United States in emphasizing cybersecurity as a national security priority. As noted by Deputy Secretary of Defense William Lynn last July, any peer state, proxy organization, or skilled group of close friends anywhere in the world with unfettered internet access is able to attack in milliseconds due to the global, open, and easy nature of the world's now huge telecommunications systems. The world of "cybered conflict" is one in which even the part-time foreign attacker can to an unprecedented degree flexibly choose the scale, proximity, and precision of any attempted attack. They can at their leisure aim at any state's military, government or commercial networks, or those of any of our allies, or associates.

Fears of more attacks are fueling a race across international defense, economic, and political communities to define and ensure national level cybersecurity. Unfortunately, relatively few understand just what "cyberspace" is, and fewer can agree on its parameters. Much of the policy and academic world has been leery of the topic because of its technical nature and most policy wonks have little idea about how networks physically work.

The Cyber Security Project

This issue brief is part of a broader effort of the Atlantic Council's project on Cyber Security. Led by the Council's Program on International Security, the Cyber Security initiative addresses emerging issues in the cyber security and defense realm, including international cooperation, private-public partnership in cyber security, as well as the role of international organizations including NATO in cyber defense and security. Under the umbrella of this initiative the Council hosts workshops, roundtables, working dinners and publishes occasional issue briefs. For more information, please contact the Associate Director of the Program on International Security, Magnus Nordenman, at mnordenman@acus.org.

The Council's work on cyber security is generously sponsored by SAIC.

Dr. Chris C. Demchak is a Strategic Researcher at the U.S. Naval War College, and received her PhD from Berkeley in political science with a focus on organization theory, security, and surprise in complex technical systems across nations. She also holds two masters degrees, respectively, in economic development (Princeton) and energy engineering (Berkeley). She has published numerous articles on societal security difficulties with largescale information systems to include cyberwar, cyber privacy, and new military models, as well as a book entitled Military Organizations, Complex Machines in the Cornell Security Studies series.

Disclaimer: Judgements made in this manuscript do not reflect the positions or policies of the US Government, the US Navy, or the US Naval War College

This level of confusion only increases the danger of serious cybersecurity surprise amidst the grand breakout of fascination, fear, and funding attached to cybered conflict. Globally dispersed cyber-rats are increasingly capable of starting cascading failures rampaging through large parts of critical national infrastructures at the scale, proximity, and precision of their choosing. They have today the patience, resources, and convenient access to exploit our cognitive, technological, and institutional disconnects from across the world's immense mass of cyber connections. As it stands, one can know only during or after the fact more or less the particulars of the opponent: who is involved, from where they launched the attack, and who might have been the intended target. Their advantage grows, the more our strategic debates remain so chaotic.

Key to this mess are two deeply buried underlying presumptions muddling debate and hence progress in the current U.S. cyber "solving" frenzy. First, it matters whether one presumes that cyberspace is completely unprecedented in human history. Second, it equally deeply matters whether the solution presumes that cyberspace is (or is not) so big as to be autonomously self-generating and thus immune to deliberate change.

If cyberspace is completely new, then the lessons of history do not help us. We need to start over in our thinking about security of a nation. If it is not, then we can extract lessons from history of conflict, people, crime, etc, to guide the creation of a cybersecurity strategy. Second, if cyberspace is now an earth-like auto-generating immune force, then the operations and importance of the cyber infrastructure are now unmanageable much like the tides or earthquakes. We can adapt ourselves to cyberspace as it evolves, but cannot change it in any major way. If it is not, then the global cyber system itself can be altered deliberately by human institutions.

Parsed across the choices, these presumptions outline four groups of strategists: cyberprophets, cyberpriests, cyberdetectives, and cyberdesigners, and, as a logical extension, four kinds of strategies now populating the miasma of conflicting voices in Washington. These are ideal types defined by their assertions in and around the cybersecurity discussions and are depicted in the table below.

Table 1.

Cyberspace Presumption	Autonomous	Not Autonomous
Totally New	CyberProphet	CyberDetective
Not New	CyberPriest	CyberDesigner

Cyberprophet

For the cyberprophet, cyberspace is both completely new and also autonomously immune to deliberate control in its growth and operation. This group has been advocating embracing the new world and its new humans for twenty years. Individuals in the 1990s began to characterize the emerging virtual world as one in which not only did history of human nature and behavior no longer matter, but that our integration of the virtual would be mutual. The underlying presumptions of newness and autonomy now live in conversations, blogs, or declarations about the vastness and inherent freedom of social networking sites and their power to change whole societies and lives. The web 2.0 and 3.0 promoters widely represent this community.

For cyberprophets, a national cyber strategy qua something one does to change cyberspace writ large is not possible and only simple adaptation is feasible. From these assumptions, society must adjust itself as good or bad events emerge, even to just enduring new levels of personal insecurity. For example, in October of 2001 Sun Microsystems CEO Scott McNealy said "Privacy is dead; get over it." For this group in its older and newer form, the best cybersecurity strategy of adaptation means selectively gating off the bad effects and trying to leave the positive interactions completely unfettered in any serious manner.

Cyberpriest

For the cyberpriest, cyberspace is autonomous in its growth and importance, but it is not completely new. Rather, it is just another expression of age-old human behaviors, needs, quirks, and frailties. While cyber priests endorse the presumption that the massive underlying telecommunications system deeply integrated with humans is now operating on its own globally, they see the threats of cyberspace as largely human in ways well known to history. Thus, like priests throughout history, they would argue for ministering to the ignorant with education and reforming the ill-behaved with information about ugly consequences. Their discussions are heavily laced with discussions of education and incentives which can banish over time the human-caused insecurities that tarnish the new era.

For the cyberpriest, appropriate cybersecurity strategies rest primarily on deterrence of bad actors, usually by persuading them of the negative consequences of hostile actions through, on, or as enabled by the cybered nets. Many senior civilian or military leaders and most of the newly arrived international relations scholars or former nuclear strategists lie in this group endorsing changing the human in ways well known. This presumption also leads to a preference to focus strategies on state-level actors and see state interests behind all major events. Deterrence works best when there is an identifiable actor on the other side, especially a state-level leader. For the cyberpriests, not knowing who attacked is especially difficult, leading to a community-wide obsession with the problem of attribution, i.e., fixing the blame when an attack occurs.

Cyberdetective

For the cyberdetective, cyberspace is all new but it is certainly not self-generating and immune to human efforts. By and large, this technologically network-savvy community built the underlying systems of the cybered world in their various professions. While impressed with their global accomplishment, cyberdetectives also see the very mechanical, programmable, and alterable underbelly of the beast. They build tools to detect anomalies or unreliabilities in their own networked operations across millions of connections in far-flung complex systems. They are not pleased to see their same tools refined by bad actors somewhere out of reach in order to cause the errors the tools were meant to identify. For this community, cyber forensics is an enormous and growing technical field now reaching out to identify bad behaviors by humans that mimic or opportunistically free ride on the normal unreliabilities of the world's cyber underpinnings. Hackers – reformed or not – inhabit this community as well. Much of the military electronic warfare community and many of the relative new transfers from sophisticated nuclear security fields fall into this group.

For cyberdetectives working in government and corporations, the strategy of choice is technological resistance. In this strategy, the goal is not to change the adversary, but to stop them technologically. Not only would attacks not make it inside the nation's critical systems, but the new systems put in place for security could reactively hit back as well. The combination of engineered software-nets-humans would discern attack paths and then guide automated or semi-automatic strikebacks to locate and disable the capabilities of attackers and/or their equipment. For both cyberpriests and cyberdetectives, attribution is a major component of their strategy for different objectives. The priests need the technology to identify the bad actors in order to understand their motives and discover ways to deter them; the detectives need the same to surveil, frustrate, or fry the equipment or skills that enable attack attempts.

Cyberdesigner

For cyberdesigners, cyberspace is neither completely new nor imperviously self-generating. This group shares a particular approach to cyberspace, viewing it as a complex socio-technical system. In this presumption, the combination and variations of networked humans and machines across cyberspace are recognizable in history and changeable in operationally critical ways. Cyberdesigners mix easily across technologically comfortable social scientists and societal systems-concerned technologists. Many of its members come from science and technology (S&T) scholars in Europe and the United States, and a number of military historians share this presumption because of their field's emphasis on the historical combinations of technology and humans in militaries. For these individuals, cyberspace is but the latest and largest iteration of such huge socio-technological systems now inserted into the foundations of modern western societies. For them, history lessons come from railroads to nuclear energy and electricity generation to global air or sea traffic controls, to how humans have adapted, derailed, or sabotaged new netted systems and to how organizations' deep institutions have responded in the past to disruptive surprises. Cyberspace is therefore something really big, but historically not all new and certainly deliberately changeable.

For this group, resilience is the best strategy by using both humans and technologies to resist some attacks, absorb and mitigate others, and reach out to anticipate and stop other attacks. The focus is on collective sense-making and knowing that a largescale, complex system can be surprising in nasty ways without an attack. The situation is simply much worse if a thinking, adjusting bad actor deliberately starts the compounding cascade of seriously disruptive events. For the cyberdesigner, resilience is constant collective learning about what socio-technical structures keep the surprises of complex systems smaller and endurable. The cyberdesigners focus on systemic human-net content-carrier pathways that can lead to cascading catastrophic military, civilian, or commercial failures. They want to know and test how those pathways are laid, explored, developed, and then used, and how socio-technical redesigns could keep the bad actors be repeatedly frustrated in their efforts, or simply stopped cold. For this community, resilience is necessary for a strike back strategy – but resilience itself does not require the intent to strike back. Rather, resilience is about exceptional command in knowledge and collective sense-making and rapid action across the systems likely to support or incur attacks.

Differing Strategies

With a millisecond attack warning framework, defining a strategy for a nation is extraordinarily challenging under any circumstances, especially so when the fundamental presumptions about what is critical are in dispute. Following the presumptions of each of these communities, the four strategies of adaptation, deterrence, resistance, or resilience, have implications for the missions, structures, and operational control of institutions required to implement each strategy. The key strategic distinctions involve the ways in which knowledge and capabilities are institutionally tied to policy preferences in restraint/deliberation, and reactive/proactive behaviors when a significant cybered surprise occurs in critical events.

Table 2.

Cybersecurity Strategies	Autonomous	Not Autonomous
Totally New	Adaptation (CyberProphet)	Resistance (CyberDetective)
Not New	Deterrence (CyberPriest)	Resilience (CyberDesigner)

A strategy emphasizing adaptation, for example, relies on restraint and mostly mitigating reaction to surprises. It means institutions would focus on understanding and plugging security holes only as they emerge and are shown to be harmful. A strategy emphasizing deterrence, however, would show restraint only technologically; with regard to possible surprises perpetrated by humans, it would be both reactive and proactive. With sting operations, cyber culture research experiments, and behavior and content surveillance, this strategy focuses on identities and motivations of possible actors for deterrence operations. Conversely, a strategy of resistance is technologically unrestrained and proactive wherever legally possible and affordable. It also involves the data from sting operations, cyber culture research experiments, and behavior and content surveillance, but this data becomes inputs to test the development of more automatic, variations of large technical solutions with as few humans as possible in the middle. Thus, while both deterrence and resistance strategies would use 'honey pots' for data on human behaviors in cyberspace, one approach would redirect people's choices, the other would rework the machines involved at any point in possible attacks.

A strategy of resilience is deliberative both technologically and socially, but it is also easily proactive in preparing to disrupt emerging attacks imposing system-wide, nasty surprises. Such a strategic emphasis means continually and comprehensively gathering data across the relevant cybered social and technical world in order to run constantly adjusted trials-and-errors and innovating to make more surprise-tolerant designs of critical human-machine interactions. Both technological and human behavior or preferences data are fodder for the constant hunt to accommodate systemically in advance those emergent interactions that could start, enhance, or even dampen the truly nasty, disruptive, cascading surprises across critical systems of a military or the nation. This strategy can also overlap with a more reactive adaptation approach when the data from systems tests suggest that the currently conceivable cascades are already accommodated by the redundancy or slack in the existing design of a system.

Large Opportunity Costs of Unresolved Presumptions

Even if the strategic debate of a large nation such as the United States can consider all four strategies simultaneously, a lack of self-awareness can lead to pernicious combinations internally in new institutions told to ensure cybersecurity. Some cybersecurity issues would have markedly different receptions according to which community's strategic emphasis is dominant in a particular security institution. A good example is the perception of the connection between cybercrime and national level cybered conflict. Cyberprophets tend to tolerate cybercrime as inevitable unless some particular exploit clearly demonstrates widespread, undisputed, and significant harm. The adaptation strategy leads the security institution to promote finding ways to live with or around the harm. The institution's actors would only seek to actively mitigate the effects of cybercrime if they seemed particularly widespread as well as nasty, and thus hard for individual adjustments. In the main, cybercrime under these circumstances would be largely ignored by the national level cybersecurity institution.

The cyberpriest tends to dismiss cybercrime as well although it expresses a human failing. Rather it is seen as a largely criminal fraud problem irrelevant to national security. In more practical terms, the cybersecurity institution strategically focused on deterrence would conclude that the criminals are too numerous and too focused on simply getting money to be effectively deterred. Furthermore, in any case, their cyber equivalent of bank robbing or mugging can be mitigated with commercial insurance and these operators are highly unlikely to want to harm the nations that provide them so much cash. For institutions guided by cyberpriests, then, international cybercrime and most of its data would be left largely to domestic police forces.

For the cyberdetective, cybercrime has mostly uninteresting, poorly skilled criminals and applications, but the emerging brilliance and threat in a particularly sophisticated new exploit is of constant interest. For example, if an exquisitely hard to detect but easy to secretly spread and powerful new innovative cybercrime program emerges globally, the cyberdetective-led institution is intrinsically focused on finding that expert cybercriminal and software author, along with the details of their exploit. The cyberdetective views such a breakthrough as something that can first emerge in cybercrime, but could easily transfer into an application used as a possible technological threat to existing resistance mechanisms for national cybersecurity. Hence, such an institution would monitor cybercrime loosely but selectively deeply forage for these hyper-skilled individuals or applications before their works spread globally.

For the cyberdesigner, however, global innovations in cybercrime are routinely of considerable interest for the nation's resilience. The cybercrime-tested range of exploits, successes, and failures across many socio-technical systems present a number of natural experiments in human-machine-networks knowledge innovation. Even low level but widespread cybercrime could have system surprise lessons. For example, quite relevant to national security would be an emergent ability of large groups of otherwise unskilled "script-kiddies" from across the globe to coordinate a mass of infected computers to aim malicious software at disrupting large regional or national infrastructure systems. For an institution with the cyberdesigner presumptions and resilience strategy, cybercrime matters because it functions as an equal opportunity, long-distance university for future cyberwarriors and their tools. The individuals and groups learn in web and real world classrooms, while the global exchange of new cybercrime applications and comments on user experiences act much like more technical lab-like experiments. Even though aimed by the cybercriminals at greed or even petty revenge, such an cybersecurity institution would constantly seek information on cybercrime in order to perceive and test any possible new set of nasty tools and surprises. The study of the complex interactions of a largescale global sandtable is necessary if these surprises are to be accommodated in advance by resilient designs of critical national systems.

Resolving the Presumptions into a Coherent Strategy

These assumptions are buried and require some self-reflection to reveal, even among the long term cyberrati. Reconciling these deep conflicts needs more progress before one locks presumptions or strategies into political and administrative concrete. And the reality of the emergent world of cybered conflict is that cyberspace is really an underlying enabler, not a dominantly people place or technical domain. Resolving the unrecognized presumptions requires capturing the real threat: rippling nasty surprising cascades near instantly disrupting critical national socio-technical needs far from the original attacks or events. Neither the cyberpriests nor the cyber detectives deal well with, respectively, the underlying technical or wider social systems. The most inclusive set of presumptions and the most system-wide strategic preferences are found in either the cyberprophet or cyberdesigner community. Of the two, however, simply adapting to nasty attacks, as cyberprophets prefer, is increasingly not politically viable, especially in the United States.

Only the cyberdesigners support a range of strategic responses to mirror the variety of social and technical undesirable surprises of cybered conflict. Their presumptions are similar to those of the cyberpriests in accepting the historical lessons of human behavior and to those of the cyberdetectives in embracing the malleability of the technologies enabling cyberspace. Only the presumptions of cyberprophets conflict directly with those of cyberdesigners. However, resilience has come to be defined in the cyberdesigner community to include processes of adaptive learning that lead to proactive innovation, thus allowing some overlap with cyberprophets at least in the strategic preference. For the cyberdesigners, responses are tailored by knowledge. Resilience may involve changing the perspectives of humans or the access points of technologies, but it may also mean unilaterally acting to change the topology of the internet if necessary for national security. Thus, the smallest of the disputing communities offers the best approach to collectively matching the complexity of the threats emerging globally.

For the future, all conflict will be cybered in major aspects, lingering with no clear end, surprising with no obvious attack mode, and often ambiguous in long-linked exchanges ranging from small to large in scale, proximity, and precision. The term 'cyberwar' with its implied end is meaningless when any enemy can be replaced without coordination by any other anywhere that the capabilities, will, and access exists. In the emerging world of always cybered conflict, the United States will need to "endure" more – strike back at enemies less – than we historically would prefer. Unfortunately, if the presumptions and focus of a chosen main national strategy do not mesh with the realities of national security in the emerging world, then the newly adapted or established national cyber security institutions will not succeed. Our national cybersecurity strategy needs to guide the emergent US Cybercommand (announced in July 2009 by Secretary of Defense William Gates) to become more a cyber 'resilience and disruption' command rather than a cyberspace-focused organization protecting or enabling traditional American military expeditionary needs. Cyberdesigners offer presumptions and the strategic preferences that most closely reflect the need to strategically embrace complexity and nasty surprises from anywhere, and still bounce forward socially and technically at the end of the day.

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN,
INTERNATIONAL
ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

CHAIRMAN EMERITUS
*Henry E. Catto

VICE CHAIRS
*Richard Edelman
*Brian C. McK. Henderson
*Franklin D. Kramer
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURERS
*Ronald M. Freeman
*John D. Macomber

SECRETARY
*Walter B. Slocombe

DIRECTORS
*Robert J. Abernethy
Timothy D. Adams
Carol C. Adelman
Michael A. Almond
*Michael Ansari
*David D. Aufhauser
Nancy Kassebaum Baker
Donald K. Bandler
Lisa B. Barry
Thomas L. Blair
Susan M. Blaustein
*Julia Chang Bloch
Harold Brown
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Sarah C. Carey
Michael P.C. Carns
*Daniel W. Christman
Wesley K. Clark
Curtis M. Coward
John Craddock
*Ralph D. Crosby, Jr.
Thomas M. Culligan
W. Bowman Cutter
Brian D. Dailey
Kenneth W. Dam
Robert E. Diamond, Jr.
Paula Dobriansky
Lacey Neuhaus Dorn
Conrado Dornier
Stanley Ebner
Eric S. Edelman
Thomas J. Edelman
Stuart E. Eizenstat
Robert F. Ellsworth
Julie Finley
Lawrence P. Fisher, II
Lucy Reilly Fitch
Barbara Hackman Franklin
*Chas W. Freeman
*John L. Fugh
Carlton W. Fulford
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
C. Boyden Gray
Marc Grossman
Stephen J. Hadley
Ian Hague
Harry Harding
Rita E. Hauser
Marten H.A. van Heuven
Richard C. Holbrooke
Mary L. Howell
Benjamin Huberman
*Robert E. Hunter
Robert L. Hutchings
Mansoor Ijaz
William Inglee
Wolfgang Ischinger
Robert Jeffrey
*A. Elizabeth Jones
Francis J. Kelly
L. Kevin Kelly
*James V. Kimsey
*Roger Kirk
Henry A. Kissinger
Philip Lader
Anthony Lake
Muslim Lakhani
Robert G. Liberatore
Henrik Liljegren
*Jan M. Lodal
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
James P. McCarthy
Eric D.K. Melby
Jack N. Merritt
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
*George E. Moose
William A. Nitze
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ana Palacio
Torkel L. Patterson
William J. Perry
*Thomas R. Pickering
Andrew Prozes
Arnold L. Punaro
Joseph W. Ralston
Norman W. Ray
Teresa M. Ressel
Joseph E. Robert, Jr.
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Matthew R. Simmons
Kiron K. Skinner
*Helmut Sonnenfeldt
Richard J.A. Steele
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
Peter J. Tanous
Peter Thomas
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Carl E. Vuono
Charles F. Wald
Jay Walker
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Dov S. Zakheim
Anthony C. Zinni

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Frank C. Carlucci, III
Warren Christopher
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS
Lucy Wilson Benson
Daniel J. Callahan, III
Geraldine S. Kunstadter
Steven Muller
Stanley R. Resor
William Y. Smith
Ronald P. Verdicchio
Togo D. West, Jr.

* members of the Executive Committee

Board list current as of April 22, 2010

The Atlantic Council of the United States is a non-partisan organization that promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org