ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

# The Five Futures of Cyber Conflict and Cooperation

The word cyberspace is nearly thirty years old,[1] and during that time, academics, theorists, and strategists have been considering how conflict will unfold in this new domain.[2] As yet, though, little has been published on what kinds of different futures may await us.[3] For example, many writers seem to imply that cyberspace itself is relatively static, when it is in fact constantly transformed through changes in usage and technology. Indeed, today's generation of digital natives has never known a world without the Internet, and their experience of cyberspace—especially in terms of security, privacy, and collaboration—will be very different from that of previous generations weaned on mainframes, modems, desktop computers, and AOL. If cyberspace is different and younger generations use it differently, then future conflict and cooperation in cyberspace may be unlike anything experienced or even envisioned by Cold War-era thinkers and strategists.

Accordingly, this Issue Brief examines five broad, possible futures of cyber conflict and cooperation over the next ten to twenty years, to ensure that we are not planning to fight—or trying to avoid—yesterday's conflict. These five possible futures are titled *Status Quo*, *Conflict Domain*, *Balkanization*, *Paradise*, and *Cybergeddon*.[4] Each is summarized in Table 1, along with an assessment of three key factors that characterize each future: how strongly the "geography" of cyberspace favors offense over defense; the intensity and kinds of cyber conflicts; and the intensity and kinds of cyber cooperation. While these five futures are not meant to be all-inclusive or taxonomic—other futures are indeed possible—these scenarios seem to cover the most interesting (and likely) grounds of conflict and cooperation.

**About the Cyber Statecraft Initiative**

The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace through global engagement and thought leadership.

This is an edited version of a paper that first appeared in a special edition on cybersecurity by the Georgetown Journal of International Affairs in 2011.

The Cyber Statecraft Initiative is generously supported by VeriSign.

## Status Quo

In a Status Quo future, conflict and cooperation in cyberspace look much the same as they do today. Despite the "geography" of cyberspace favoring offense over defense, cyberspace is generally a safe place in which to do business and to communicate with others, even though criminals continue to engage in multimillion-dollar heists and steal millions of people's personal details; national foreign intelligence agencies poke and prod for military and industrial

1 Having been coined by William Gibson in his short story, "Burning Chrome," in 1982, and popularized in *Neuromancer* in 1984.

2 Such as in Winn Schwartau's seminal *Information Warfare: Chaos on the Electronic Superhighway*, in 1994.

3 One exception is CISCO's excellent "The Evolving Internet: Driving Force, Uncertainties and Four Scenarios to 2025" (2010); however, this report focuses primarily on technology and usage, rather than on national-security conflict and cooperation.

4 For a more detailed examination of particular scenarios that illustrate how offensive cyber operations might be used in a conflict, see Greg Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," *Proceedings of a Workshop on Deterring Cyberattacks*, National Research Council (2010).

**Jason Healey** is the Director of the Cyber Statecraft Initiative at the Atlantic Council of the United States. You can follow his comments on cyber issues on **Twitter at @Jason_Healey**.

**Table 1: Comparison of Possible Futures of Cyber Conflict and Cooperation**

| | Status Quo | Conflict Domain | Balkanization | Paradise | Cybergeddon |
|---|---|---|---|---|---|
| **Description** | Cyberspace conflict tomorrow looks like that of today: there are high levels of crime and espionage, but no massive cyber wars. | Cyberspace has a range of human conflict, just like air, land, space, and maritime domains. | Cyberspace has broken into national fiefdoms: there is no single Internet, just a collection of national Internets. | Cyberspace is an overwhelmingly secure place, as espionage, warfare, and crime are extremely difficult | Cyberspace, always un-ruled and unruly, has become a "failed state" in a near-permanent state of disruption. |
| **Relationship of Offense and Defense** | **Offense** > Defense | **Offense** > Defense | Unknown/Depends | **Defense** >> Offense | **Offense** >> Defense |
| **Intensity and Kind of Conflict** | Conflict is as it is today: bad, but not catastrophic, with crime and spying. | There is a full range of conflict: crime, spying, embargos, and full-blown international conflict. | Nations are possibly blocking access to content, to and from each other, although there may be fewer outright attacks. | All conflict is greatly reduced, although nations and other advanced actors retain some capability. | Every kind of conflict is not just possible, but ongoing, all of the time. |
| **Intensity and Kind of Cooperation** | There is a healthy but limited sharing on response, standards, and cyber crime. | To be stable, cyber cooperation requires norms and regimes, just as in other domains. | Cyber cooperation requires international agreement in order to interconnect national Internets. | Cooperation is critical if stability depends on norms, or unneeded if it depends on new technology. | Cooperation is either useless, as attackers always have the edge, or impossible, like trying to govern a failed state. |
| **Stability** | Relatively Stable | Relatively Stable? | Unknown/Depends | Long-Term Stable | Long-Term Unstable |
| **Likelihood** | Moderate | High | Low | Low | Low |
| **Why This Is Possible** | Current trend line and massive attacks have not occurred yet, despite fifteen years of expectations. | Other domains have generally supported a range of human activity, from commerce to conflict. | Countries continue to build border firewalls, which UN control of the Internet could exacerbate. | New technologies or cooperation, long promised, could make security much easier. | Offense continues to outpace defense, as any new defensive technology or cooperation is quickly overcome. |

secrets; denial-of-service attacks are capable of disrupting nearly any target; and militaries make plans to unleash organized cyber violence, if called upon.

The system remains stable overall, despite discontent, difficulties, and disruptions. People tweet, Skype, listen to music, wander Wikipedia, and play World of Warcraft. Businesses rely on cyber connections to produce and deliver their goods and services, and depend on e-mail and web presence to communicate with their clients. Governments depend on Internet-delivered services, and some, like Estonia, even have elections online.

It is possible, though not likely, that our cyber future will look like the cyber past and present. Since the dawn of cyberspace, experts have predicted that a catastrophic attack was imminent, yet nearly two decades along, all of its major disruptions have been lacking in scope, duration, and intensity. Although cyber war has loomed, it has not yet materialized. If it turns out that this has not been merely luck, but some kind of underlying stability,[5] then it is entirely possible that Status Quo will be our cyber future.

5 Such as, if strategic disruption of cyberspace turns out to be especially difficult to accomplish; this might be the case if strategic attacks are particularly hard to execute, or defenses are more resilient than expected. See Gregory Rattray's *Strategic Warfare in Cyberspace*, chapters 3 and 4, for a more detailed analysis.

## Conflict Domain

If cyberspace becomes a Conflict Domain, cyber terror and cyber war, which in 2011 are more hyperbole than fact, will become reality.

Cyberspace will contain not just the malicious actions and actors we see in a Status Quo future, but also the full range of conflict we see in the other "war-fighting domains" of air, land, space, and maritime. It will become as common to have militaries attacking each other in cyberspace as it is in the "real" (non-cyber world). These attacks will include attacks integrated into traditional "kinetic" operations as well as in large-scale cyber-on-cyber attacks. Terrorists, in addition, will embrace the new avenues of attack, realizing that they can achieve both disruptions and headlines. There will not only be "digital Pearl Harbors" and "digital 9/11s," but also digital "Battles of Britain" and "Battles of St. Mihiel" and every other kind of digital conflict,[6] many of which are only imagined today by science-fiction writers.

Moreover, just as somewhere in the world there are many large-scale physical conflicts, the world will become used to there being many ongoing cyber conflicts, some of them lethal. Indeed, it will be uncommon for there to be a conflict that does not have an online component.

Despite this flurry of organized and unorganized violence, cyberspace will remain generally as stable as the air, land, space, and maritime domains. The residents of cyberspace—mostly very young and very adaptable—gradually learn to work through the crime and disruptions, so the Internet remains a relatively trusted place for communication and commerce. There may be certain areas equivalent to modern-day Somalia—dangerous to be in, or even near—but these "failed" regions of cyberspace are widely known to be dangerous, and most people can easily avoid them. Accordingly, damaging attacks are unable to cause widespread instability throughout cyberspace for long periods of time.

Cooperation in a Conflict Domain future will require grounding in the norms and regimes that have helped to tame conflicts in other domains: transparency, confidence-building measures, formal and informal treaties, and laws of armed conflict. Some—perhaps even most—of these norms and regimes can be borrowed directly; others will have to be adapted or invented.

How might this future come about? In 1995, the Air Force described just how it was even then emerging:

> Before the Wright brothers, air, while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical.[7]

Conflict Domain is the most likely cyber future, and in many ways, the default future. Assumedly each and every adversary in cyberspace is working to improve its capability, and many (at least organized-crime groups, militaries, and terrorists) seek to be able to have long-lasting and wide-reaching effects, whether in stealing money or information, or in disrupting their enemies. And so it seems that there are three scenarios in which we would *not* find ourselves in this future: first, cyberspace would somehow be more resilient to attacks than is currently expected, so that large-scale military operations could not easily happen—in which case we would likely be in Status Quo or Balkanization. Second, defensive techniques or technology would shift the geography strongly in favor of the defenders, putting us in Paradise. Or, finally, the attackers would operate with such impunity that our future would be Cybergeddon.

## Balkanization

In the Balkanization future, different actors in cyberspace—predominantly, nations—would build sovereignty and borders so that there would no longer be a single Internet, but a collection of smaller Internets. As expressed by one academic: "Just as it was not preordained that the internet would become one global network where the same rules applied to everyone, everywhere, it is not certain that it will stay that way."[8]

Nations are erecting national firewalls and virtual borders to information and it is possible that this emerging collection will

6 A more complete categorization of operational possibilities for offensive cyber operations can be found in "Categorizing Offensive Cyber Operations" by Greg Rattray and Jason Healey, in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies of Science (2010).

7 Department of the Air Force, Cornerstones of Information Warfare, Department of Defense, Washington, DC (1995), available at **www.iwar.org.uk/iwar/resources/usaf/iw/corner.html**, accessed on May 13, 2011.

8 Kevin Werbach, quoted in *The Economist*, "The Future of the Internet: A Virtual Counter-Revolution," September 2, 2010.

be enough to partition the current Internet. China and Russia seem to be trying to build a system for permanently prohibiting access to selective parts of the Internet while others (like Egypt and Libya did in early 2011) may decide to "turn off" the Internet (at least temporarily) within their borders. These regimes showed that nations have and may again prefer no Internet to an open Internet if they are in peril. These borders ironically had their start with France over a decade ago and Western democracies increasingly support limited borders to prevent child pornography or protect intellectual property.[9]

The effect of these borders could be to transform the Internet. Rather than being one global network, the future Internet might become fragmented like the telephone system. Each nation would have full control over its own telephone lines and come together, through the United Nations' International Telecommunication Union, to agree on how to exchange international traffic.

In a Balkanized future, nations would find it easier to clamp down on the right of freedom of opinion and expression "through any media and regardless of frontiers," as codified in the 1948 Universal Declaration of Human Rights.[10] Some nations are already displaying a strong trend in this direction, as can be seen in an official agreement by the Shanghai Cooperation Organization (SCO), comprised of China, Russia, and Central Asian nations. In a 2008 declaration,[11] the SCO—alongside other "main threats" to information security, like information weapons, crime, and information terrorism—expressed their worry about the "use of the dominant position in the information space to the detriment of the interest and security of other States . . . [and] dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States." If CNN or Facebook are threats, then strong national firewalls cutting off other nations and blocking harmful content could be an extremely valuable tool.

One way such a future might emerge is through United Nations control over core Internet functions, such as those run by the Internet Corporation for Assigned Names and Numbers. Currently, this group (though still partially connected to the US government) uses a process in which states have a voice, as do individuals, corporations, and nonprofit groups. If this "multi-stakeholder" process were supplanted by one centered on the UN—such as with the telephone system—then every nation would have an equal vote, with no official voice for anyone else. This would open the possibility of allowing more repressive nations to run the Internet as they see fit. Robert Knake, then of the Council on Foreign Relations, summarized the dilemma this way in 2010:

> If the current Internet is a reflection of the openness and innovation that are hallmarks of American society, the Internet of the future envisioned by Russia and China would reflect their societies—closed, dysfunctional, state-controlled, and under heavy surveillance.[12]

A Balkanized Internet may actually improve many of the current security problems of cyberspace, as nations would have more levers available to stop all kinds of unpleasant traffic. This would, of course, be matched by limits on cross-border speech and commerce, however, so most Western societies would be unhappy with the resulting trade-offs.

## Paradise

In the Paradise future, cyberspace would become radically safer and more secure either through revolutionary new technologies, or through an accretion of small changes in technology and practices. Instead of the "geography" of cyberspace favoring offense over defense—as in Status Quo, Conflict Domain, and Cybergeddon—in a Paradise future we would have a cyberspace where the defense is far superior to the offense. It would simply be very difficult for most cyber actors to achieve any malicious aims. Nation-states—or other very well-funded and patient organizations—would still be able to operate, albeit with greatly reduced operational flexibility, and they would not be able to threaten the long-term stability of cyberspace as a whole.

9 See Who Controls the Internet? by Jack Goldsmith and Tim Wu on how France began the move for Internet borders with a legal case against Yahoo! As an example of current Western borders, the Australian national cyber strategy groups any steps to protect their populace from Internet content (like online pornography or bullying) as "cyber safety".

10 United Nations, Universal Declaration of Human Rights, Article 19 (1948), from **www.un.org/en/documents/udhr/index.shtml**.

11 Shanghai Cooperation Organization, "Agreement between the Members of the Shanghai Cooperation Organization on Cooperation in the Field of Information Security," 61st Plenary Meeting, December 2008.

12 Robert Knake, "Internet Governance in an Age of Cyber Insecurity," Council on Foreign Relations, Council Special Report #56 (2010).

The Paradise future is possible, but not likely, requiring either a tremendous number of small things to work well enough, or one or two tremendously large ones to work perfectly. In the past, many new technologies have been created with the goal of ensuring a secure Internet. Some of these technologies were devices (e.g., firewalls or intrusion-detection or prevention appliances), and others were standards (such as secure versions of the Internet Protocol or Domain Name System) or software (host-based behavior blockers). While no technologies, alone or in combination with others, have delivered Paradise yet, it is certainly conceivable that it will happen in the middle future. For example, the scourge of syphilis and countless other diseases were cured after one small discovery: Alexander Fleming's isolation of penicillin. Perhaps an equivalent discovery that will shift the balance in favor of cyber defenders is near.

Of course, it is not just through new technology that we could smother nearly all attacks. Cyberspace might just be able to settle into long-term stability if people, organizations, and nations had the will to make different decisions and take smarter actions. Such decisions and actions might include companies, governments, and individuals keeping their systems well patched. Also, Internet service providers could clamp down on denial-of-service attacks (or other obvious malicious traffic).

It might turn out that such simple actions could have a disproportionately beneficial effect: Verizon reported that out of 800 criminal incidents investigated in 2010, fully 92 percent were "not highly difficult," and 96 percent could have been prevented with simple or intermediate security controls.[13] Similarly, according to a survey by Arbor Networks, 27 percent of network operators do not attempt to detect outbound or cross-bound attacks, and, of those that do, nearly half take no action to mitigate such attacks.[14] Stopping these incidents and attacks would not be able to stamp out true "cyber warfare" (any more than you could build a ship so invulnerable that it could never by sunk by a determined adversary), but they are relatively easy and would be important first steps toward a Paradise future.

## Cybergeddon

In Cybergeddon, the worst future of them all, the unruliness of cyberspace has gained the upper hand, further shifting the geography so that the offense now has an overwhelming, dominant, and lasting advantage over the defense. Attackers—whether hackers, organized-crime groups, or national militaries—can achieve a wide range of effects with very little input, making large-scale, Internet-wide disruptions easy and common. Every kind of conflict is not just possible and occurring (as in Conflict Domain), but they seem to be occurring all the time. Moreover, cyberspace is no longer a trusted medium for communication or commerce, and is increasingly abandoned by consumers and enterprises. Worse yet, all attempts to invent new, more-secure technologies or standards are soon swamped by attacks as well, defying attempts to redress the balance. Cooperation among nations, or with nongovernmental organizations, is similarly useless—either because there is rampant mistrust between participants, or because attackers are ubiquitous, relentless, and triumphant.

CISCO, in its excellent report on "The Evolving Internet," also sees Cybergeddon as one of the possible Internet futures, calling it "Insecure Growth":

> This is a world in which users—individuals and business alike—are scared away from intensive reliance on the Internet. Relentless cyber attacks driven by wide-ranging motivations defy the preventive capabilities of governments and international bodies. Secure alternatives emerge but they are discriminating and expensive.[15]

Though such a future may sound unbelievable, there is at least one similar example in other domains. The US military is already tracking 20,000 objects in orbit (expected to triple by 2030), and this space-debris problem may already be past the "point of no return." The situation is not unstable yet, but is likely to be soon, when "operational satellites will be destroyed at an alarming rate, and they [will not be able to] be replaced."[16] In such a future, resources in space could no longer be trusted, a situation which could last decades.

13 Verizon Data Breach Investigations Report (2011), p. 3.

14 Arbor Networks, "Worldwide Infrastructure Security Report: 2010 Report," Vol. 6, pp. 15–16.

15 CISCO, "The Evolving Internet: Driving Force, Uncertainties and Four Scenarios to 2025" (2010), p. 19.

16 Quote from Marshall Kaplan, orbital debris expert, from "Ugly Truth of Space Junk: Orbital Debris Problem to Triple by 2030," Space.com (May 9, 2011).

Although the Cybergeddon future is not likely, it is far from impossible. While someday a non-state organization may someday have the means and ruthlessness to destroy a decisive part of our information based society, perhaps the only required enabler Cybergeddon needs is continued lassitude. Governments and individuals have long made the lazy choices rather than heed the many warnings of imminent catastrophe in cyberspace.

## Conclusion

It is in the long-term interests of the United States and other like-minded nations to seek a future of Paradise in cyberspace, one that has long-term stability and neutralizes all but the most cunning and determined attackers. Such a future protects American commerce and freedom of speech while still granting the US military options to use cyber capabilities to supplement or replace kinetic firepower. A Paradise future is also likely in the interest of nations that are not liberal or democratic. China will forego much of its potential international leverage and influence in a Balkanized future, as many nations might reciprocate against Chinese information blockades.

Fortunately, the steps needed to create the most desirable Paradise future are largely the same that are needed to avoid the least desirable, Cybergeddon, and, as luck would have it, these steps have for years been detailed by many groups, commissions, and experts. All that is required is to find the will to implement these recommendations. These include quickly patching vulnerable or infected computers, making it difficult for attacks to transit the core networks, and engaging in a dialogue with international partners to find areas of common concern and mutual action. Hopefully, recognizing these possible futures will make it more likely that we can safely navigate toward the one we desire rather than the one we currently deserve.

*DECEMBER 2011*

# The Atlantic Council's Board of Directors

## CHAIRMAN
*Chuck Hagel

## CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

## PRESIDENT AND CEO
*Frederick Kempe

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

## TREASURERS
*Ronald M. Freeman
*John D. Macomber

## SECRETARY
*Walter B. Slocombe

## DIRECTORS
*Robert J. Abernethy
Odeh Aburdene
Timothy D. Adams
Carol C. Adelman
Herbert M. Allison, Jr.
Michael A. Almond
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
Ziad Baba
Ralph Bahna
Donald K. Bandler
Lisa B. Barry
*Thomas L. Blair
Susan M. Blaustein
Julia Chang Bloch
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Daniel W. Christman
Wesley K. Clark
John Craddock
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula Dobriansky
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Eric S. Edelman
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Barbara Hackman Franklin
*Chas W. Freeman
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*C. Boyden Gray
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Harry Harding
Rita E. Hauser
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Benjamin Huberman
Linda Hudson
*Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly
L. Kevin Kelly
Zalmay Khalilzad
Robert M. Kimmitt
James V. Kimsey
*Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
Muslim Lakhani
David Levy
Henrik Liljegren
*Jan M. Lodal
George Lund
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
Eric D.K. Melby
Rich Merski
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Sean O'Keefe
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ahmet Oren
Ana Palacio
Torkel L. Patterson
*Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Norman W. Ray
Teresa M. Ressel
Joseph E. Robert, Jr.
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Harry Sachinis
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Kiron K. Skinner
Anne-Marie Slaughter
Alan Spence
John M. Spratt, Jr.
Richard J.A. Steele
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael Walsh
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
Harold Brown
Frank C. Carlucci, III
William J. Perry
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
Henry E. Catto
Kenneth W. Dam
Stanley Ebner
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
Stanley R. Resor
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

**Members of the Executive Committee*
*List as of October 28, 2011*

The Atlantic Council is a non-partisan organization that promotes constructive US 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**