Civilian Research Project

Forming a Cyber Coalition

By

Colonel Terrence L. Howard
United States Army

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
06-04-2012	Civilian Research Paper	June 2011 – May 2012

4. TITLE AND SUBTITLE

Forming a Cyber Coalition

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Terrence L. Howard

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Senior Service College Fellowship Program
The University of Texas at Austin
1 University Station, G1000
Austin, TX 78712

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Ave.
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: UNLIMITED

13. SUPPLEMENTARY NOTES

None

14. ABSTRACT

The public-private sector, international organizations, states, non-state players and adversaries increasingly rely on the cyber space environment for trade, socialization, commerce and the free flow of information. Any significant disruption in cyber space poses a considerable risk to our political, social, and economic systems. With the steady rise of cyber attacks, the international community coupled with numerous state and non-state players face the grim reality that cyber terror is the new weapon of choice. Establishing a coalition of like-minded cyber partners to address international laws, privacy, and intelligence sharing is paramount to our success and protection. I will discuss proven techniques used by battle field commanders to prepare their formations for conflict and contrast those techniques with the cyber community's actions to deal with cyber terror.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	18	

USAWC CIVILIAN RESEARCH PROJECT

FORMING A CYBER COALITION

by

Colonel Terrence L. Howard
United States Army

Dr. William Young
Project Adviser
University of Texas at Austin

This Civilian Research Paper is submitted in partial fulfillment of the Army War College Fellowship Program. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

FORMING A CYBER COALITION

The public-private sector, international organizations, states, non-state players and adversaries increasingly rely on the cyberspace environment for trade, socialization, commerce and the free flow of information. Currently it is estimated that over 2 billion people are connected to the cyber world.[1] Users of cyberspace have developed a quasi sense of entitlement with relatively free rein to operate e-globally and at will. There is a general belief that cyberspace will be there and largely available for everyone to use and enjoy. That assumption contrasts with the grim reality of the growing cyber threat across social, political and economic boundaries. The US government responded to the threat of cyber space terror by releasing the Department of Defense Strategy for Operating in Cyberspace in July 2011. This strategy outlined five Strategic Initiatives to deal with the increasing vulnerabilities of the electronic information age. Strategic Initiative Four directs the establishment of bilateral and multilateral partnerships with like-minded nations.[2] With so many networks, nations, and peoples connected to cyberspace, the initiative is ambitious and very much needed. It is important to note that more laws, more firewalls, more defenses, more protectionist actions will not solely combat the threats within cyberspace. Thus, Strategic Initiative 4 must succeed in uniting those that are 'willing & transparent' cyber partners with those that are 'unwilling & translucent' with their partnership.[3] To accomplish this we must understand the motivations of our like-minded partners while enticing our unlike-minded members to find the optimal Collaboration Target Zone in forming CyberCo (Cyber Coalition of the Willing/Unwilling).[4]

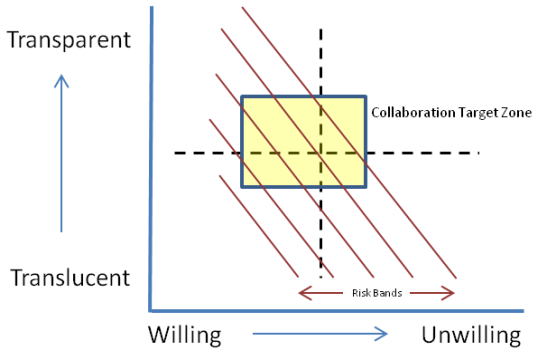

Figure 1: Collaboration Target Zone

Cyber bilateral and multilateral agreements must incorporate and accomplish the needs of all by successfully achieving appropriate defensive and offensive actions to protect the digital world without digital Darwinism, whereby the survivors are typically the loudest and the most opinionated.[5] Arguably we can assemble the brightest minds in the world to find ways to technically harden cyberspace from vicious intenders. Such a draconian measure would defeat the purpose of an open electronic environment, however, and the unintended consequences are yet to be fully understood. A cyber coalition must incorporate policy and laws that respect the rights of individuals and groups to use the World Wide Web while simultaneously protecting them from borderless cyber threats. Consider the actions of a commander before a military operation. An intelligence-assessment of the battle space is developed and approved by the commander. The intelligence-assessment serves as a guide for war fighting formations to prepare for contingency operations. Coalition partners need the same approach for defining a comprehensive solution for all in defeating malicious intenders in the cyber world. As depicted in Figure 1 above, defining and understanding the collaboration target zone would greatly enhance the coalition's conventions to combat cyber terror and threats.

The Estonia Effect

To gain a better appreciation for the challenges that lay before this cyber coalition, rewind to April 2007 in the country of Estonia. The Estonians were victimized by a wave of relentless electronic assaults against their public and private network infrastructure. Although there have been many cyber attacks before this incident, this was the first time that a sovereign nation was attacked via cyber space. Arguably Estonia continues to serve as the model nation for their IT infrastructure and efficiencies in e-State and e-Commerce. Their advancement in

cyber security and information technology, arguably, rivals many well established and developed nations. Consider these facts in 2007 for Estonia[6]:

- 98% of Estonian's territory was covered with Internet access: fixed line, broadband, WiMax, WiFi, and CDMA21 mobile wireless Internet access solutions
- mobile phone penetration was nearing 100% with a few rare exceptions due to landscape challenges
- 50% of the population age 16-74 were active internet users
- e-State information administration systems provided more than 1,000 unique electronic services online
- first country to introduced electronic voting for state elections
- 95% of all banking transactions were conducted electronically
- electronic mobile-parking accounted for 50% of all fees collected for parking

Estonia emerged from the cyber attacks with a strengthening resolve to implement more effective cyber security measures at home and abroad. In 2008 the Estonia Ministry of Defence released their cyber security strategy. The strategy noted five policy initiatives for enhancing cyber security: the development and large-scale implementation of a system of security measures; increasing competence in cyber security; improving the legal framework for supporting cyber security; bolstering international co-operation; and raising awareness on cyber security. In an effort to bolster international cooperation their policy aims to:[7]

- recognize cyber attacks as a moral condemnation against life, human rights and democratic freedoms
- actively participate in developing and implementing international cyber security policy
- promote the adoption of international conventions against cyber crimes and attacks
- develop cooperative networks for cyber security

The Estonian government quickly recognized the importance of establishing cooperative partnerships and coalitions to combat cyber terrorism. Although the other four policy initiatives are vital to Estonia's success, they are beyond the scope of this paper.

Cyber attacks transcend all perceived borders and boundaries. According to the Office of Management and Budget's (OMB) Fiscal Year 2010 report, the United States Computer

Emergency Readiness Team (US-CERT) recorded an increase in attacks on private and public information technology (IT) systems by 39% from the previous year.[8] No individual, group, industry, state nor non-state player is immune to cyber threats. Cyber warfare is a component of the ongoing struggle between philosophies of politics, governance, and markets to be waged by opposing interests, be they nation versus nation, law enforcement versus criminals, religion versus the world, or security forces versus terrorists.[9] Consider the possible reasons behind these cyber attacks:

- May 21, 2011 – Lockheed Martin, the world's largest aerospace manufacturer and the top supplier to the Pentagon, discloses a high-level security attack against information systems.[10]
    - Possible reason – competitors and/or nations want aerospace technology/information without the research and development cost burden

- Fiscal Year 2011 – A Department of Energy (DOE) Audit reports on a successful cyber attack but did not release any additional details. The DOE has dozens of agencies, regional offices and laboratories to include the U.S. nuclear weapon stockpile.[11]
    - Possible reason – terrorist are interested in the US nuclear arsenal

- September 26, 2011 – Harvard University's website was attacked by an alleged criminal tied to the Syrian regime. The hacked homepage displayed a prominent image of Bashar al-Assad, the President of Syria, with a text proclaiming "Syrian Electronic Army Were Here".[12]
    - Possible reason – Syrian sympathizers want to send a message/warning to one of the most prestigious academic establishments in the world

- January 25, 2012 – Two Israeli medical centers, Tel Hashomer and Assuta were attacked. This attack is only the latest in a strike-counterstrike series of online skirmishes between Israeli and Arab hackers that began when a Saudi hacker published Israeli credit card data online.[13]
    - Possible reason – byproduct of the ongoing hatred between the Arab and Jewish communities

- June 14, 2011 – A likely spear-phishing attack was specifically targeted to give a nation state a 'digital insider presence' into the International Monetary Fund (IMF) network. The breach prompted the World Bank to cut its computer link to the IMF.[14]
    - Possible reason – non-state and/or state players want information that may support or deny Greece an economic bailout

Cyber crimes are as much an international challenge as they are a national challenge. Great strides have been made to bolster laws and policies to combat and prevent attacks. However it is tough to agree on what constitutes cyber mischief within a coalition of willing partners and probably much tougher to come to agreements with less-willing participants. For the purpose of this research paper less-willing participants include individuals, groups, companies, non-state and/or state players willing to listen/engage/implement policy yet act independent of the coalition. The un-willing participants include rouge states, non-state players, morally corrupt societies/groups, those with extreme ideological views, and all others un-willing to conform to the norms and rules of the cyber coalition. It is reasonable to assume that un-willing participants will not engage with the coalition to establish policy and share technical ideas in any given situation. Therefore un-willing participates are beyond the scope of this paper.

Simulation and International Participation

The North Atlantic Treaty Organization (NATO) took up the cyber security cause and established the Cooperative Cyber Defence Centre of Excellence in Estonia. As outlined in Estonia's Cyber Strategy, international cooperation is critical to successfully combat cyber threats. Laws, regulations, and policy issues must be addressed, resolved and enforceable in order to share and harden the coalition's cyber offenses and defenses.[15] Historically looking back at other international rules of law it is reasonable to conclude that cyber enforcement will be more challenging given its borderless nature and anonymity. In July 2004 the Convention on Cyber crime was adopted as the first international treaty to address computer and internet criminal activity. This Convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[16] As of October 28, 2010 thirty states

signed, ratified and acceded to the convention, while sixteen additional states signed the convention without ratification.[17] Ratification of the law is essential to border enforcement and mutual cooperation across sovereign borders. However without a nation's ratification of a cyber crime law, countless people will be victimized by cyber crimes without the fear of retribution.

Battlefield commanders prepare their formations through constant training and retraining to the threat. Rigorous battle-drills, simulation exercises and war-games are excellent training tools used to assess the state of readiness for the unit. Much like our battlefield commanders, cyber coalitions must train and retrain proven techniques to deal with this new age of cyber weaponry. Twenty months after a cyber war was declared on Estonia, the Business Executives for National Security (BENS) sponsored Cyber Strategic Inquiry 2008 (CSI'08). CSI'08 gathered more than two-hundred thirty leaders from government, industry and society to focus on cyber security risks and potential solutions for the United States. Leaders were exposed to multiple cyber attack situations and events which heighten our confusion and doubt about our nation's ability to function in a cyber attack. It was clear that the collective community was ready to neither combat nor prevent the perils of a cyber attack. The take-aways from CSI'08 included:[18]

- establish clear lines of authority for planning and executing a cyber mission
- expand the legal frameworks to support full-spectrum cyber security challenges, including the balancing of privacy with information sharing
- evolve thinking to include risk management and resilience
- develop and implement a flexible response plan to effectively manage cyber security and facilitate public awareness and education
- recognize the need for cooperation among government, industry and society
- leverage innovative technologies and the unique capabilities of government, industry, academia and the broader society

Fourteen months following BENS's CSI'08, Cyber Shockwave, another cyber simulation exercise, was conducted on February 16, 2010. The Cyber Shockwave simulation concluded

many of the same findings from CSI'08. Simply stated, the United States was still unprepared for a catastrophic cyber attack. The take-aways included:[19]

- a need for well-defined responsibilities for maintaining situational awareness
- establish an effective decision-making framework below the Cabinet level
- incorporate a user-friendly process for collaboration between government and private sector teams

Building on lessons learned from previous simulation exercises, the National Cyber Center Division of the Department of Homeland Security sponsored a three-day international cyber simulation exercise on September 27, 2010 called Cyber Storm III. Thirteen countries, eleven states and seven US federal agencies participated in the exercise designed to assess the operational capabilities and the broader information sharing practices of the participants during an escalating cyber attack scenario. According to Bobbie Stempfley, director of Homeland Security's National Cyber Security Division, this exercise will help determine where the kinks are in the National Cyber Incident Response Plan (NCIRP).[20] NCIRP establishes the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident. It ties various policies and doctrine together into a single tailored, strategic, cyber-specific plan designed to assist with operational execution, planning, and preparedness activities and to guide short-term recovery efforts.[21] Like our battlefield commanders, these cyber simulations were instruments of change needed by the international community to further emphasis the importance of fighting the cyber threat together.

Complexity of a Cyber Coalition

As stated earlier, battlefield commanders use an intelligence-assessment to guide, train and prepare their formations for battle against an often known adversary. Defining cyber terrorism has proven to be much more difficult and often very controversial. Consider the following operational definitions of cyber terrorism:[22]

- United States Federal Bureau of Investigation: The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
- The United States Department of Defense: The unlawful use of, or threatened use, of force or violence against individuals or property, to coerce and intimidate governments or societies, often to achieve political, religious or ideological objectives.
- The United States Department of State: Premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents.
- Dr Dorothy E. Denning, Professor of Computer Science at Georgetown University: Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

There are hundreds of definitions for cyber terror. The international community and many nation-states struggle to fully embrace a single definition. Historically, societies have used internal (law enforcement) and external means (international agreements or military operations) to maintain social order for human survival and prosperity. Societies enforced and defended sovereign borders and identified the threats as internal or external.[23] The cyber world transcends this classical thinking by expanding ideology, politics, and commerce into a borderless sphere. Cyber terrorism can be launched from virtually anywhere in the world. It literally resides unregulated between societies' internal and external enforcement. This dichotomy has created a cyberistic abyss. Considering the complexities associated with any single definition, the motivations of individuals/groups/nations and the speed of new technologies introduced to the cyber lexicon, I would submit that it is in our collective best interest to avoid taxonomy on cyber terrorism. Put the coalition's energy and resources into: awareness, aggressive defensive and

offensive operations, intelligence sharing (technical and non-technical), and more legal discretion related to cyber space threats/crimes. A definitive definition of cyber terrorism limits a coalition and a nation from having the necessary flexibility to resource, preemptively respond and defend against cyber threats. Without question there must be oversight for these board legal discretions. Avoiding a single definition will require flexibility, innovation and cooperation among like-minded nations.

As shown in Figure 2 cyber attacks are on the rise and the offenses are more complex and more brazen than ever before.[24] Non-state actors are playing an increasing role in cyber space especially with respect to: cyber crimes, cyber espionage, and cyber warfare.

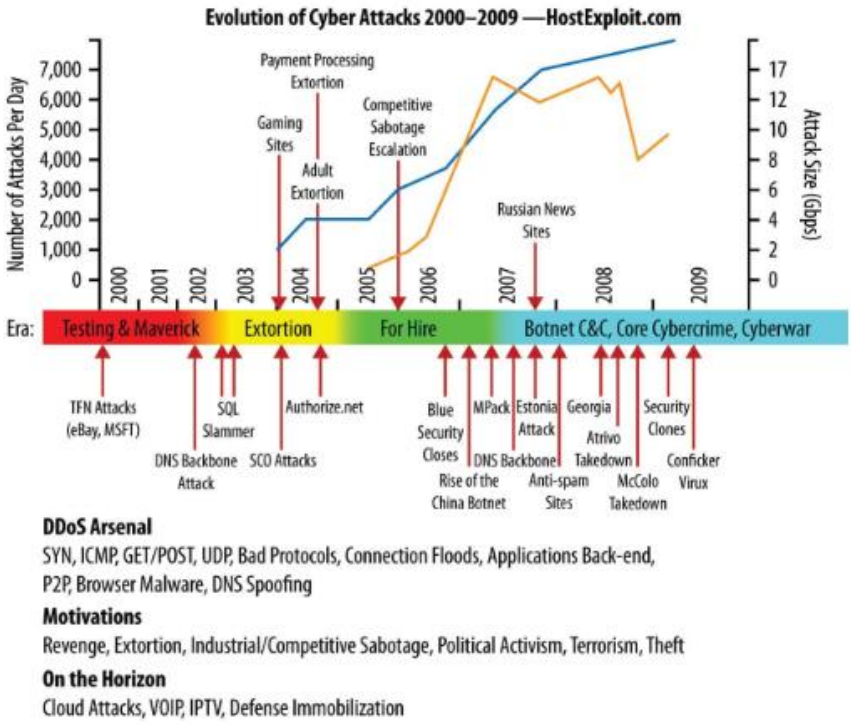

Figure 2: Evolution of Cyber Attacks

The anonymity of cyberspace has proven to be troublesome in assigning attribution.[25] Governments can secretly impose their will on their adversaries while maintaining plausible denial of any involvement in a cyber attack. Consider the following coincidences and draw your own conclusions about state supported hacker activities:[26]

- China: An estimated 3,000 hackers self-organized into a group called the China Hacker Emergency Meeting Center and launched attacks against several Indonesian government websites in response to anti-Chinese riots that took place in May 1998.

- May 1999 a NATO jet accidentally bombed the Chinese embassy in Belgrade, Yugoslavia. Within a few short hours the Chinese Red Hacker Alliance attacked hundreds of US government websites.

- In 2001 when a Chinese fighter jet collided with a US military aircraft over the South China Sea, approximately 80,000 hackers engaged in "self-defense" cyber war for what they deemed to be an act of US aggression.

- Russia: The Russian military invaded the breakaway region of Chechnya to reinstall a Moscow-friendly regime. Both sides used cyberspace to engage in information-operations to control and shape public perception. After the war ended, the Russian Federal Security Service (FSB) was reportedly responsible for knocking out two key Chechen websites at the same time that Russian Spetsnaz troops engaged Chechen terrorists who were holding Russian civilians hostage in a Moscow theater in October 2002.

- North Korea: In 2009 several websites in the United States and South Korea were allegedly attack by the Democratic People's Republic of Korea (DPRK). Despite empirical evidence of responsibility, North Korea has ignored pressure from the South Korean media and government officials for a response. Congressman Pete Hoekstra (R-MI) further called for the US military to launch a cyber attack against the DPRK to send them a "strong signal."

- Iran: The Stuxnet computer worm was secretly launched in 2009. It was designed to damage centrifuges at a uranium enrichment facility in Iran. Experts concluded that this worm was state sponsored. Israel and/or the United States are allegedly aware of the details.[27]

It can be argued that non-state cyber actors are becoming a protected asset which further hurts the cyber coalition of the willing. Despite the belief that a significant portion of the hacking activities against the United States reside within Chinese and Russian borders, neither China nor Russia have taken aggressive and active measures to prosecute online attackers unless those attackers targeted companies within their borders.[28]

The nature of international leadership within the United Nations (UN) has greatly transformed since the Cold War. There is a greater push to expand the role of global governance, yet the challenges and differences are more pronounced than ever before. As an example, consensus-building, governance and the negotiation of rules based on transparency and

accountability remain formidable obstacles within the UN.[29] Although the United States continues to benefit from the privileges associated with hegemony, rising powers are seeking new opportunities to gain or at least erode the United States' global influence. Countries and regions are incorporating alliances and economic agreements outside of organizations like the World Trade Organization. These regional and political alliances will further erode the coalition's ability to organize for success. James Reed takes this argument a step further by suggesting and defending an argument that it is in fact the United States that lacks in ability to be like-minded.[30]

Role of the Private Sector and Trust

> "The international policy-making stage is increasingly congested with private and public non-state actors jostling alongside governments in setting and implementing the agenda of the new century. The multitude of new actors adds depth and texture to the increasingly rich tapestry of international civil society."[31]

The internet started as a Department of Defense project that allowed connected computers to communicate and share information. This technology quickly grew into what we know as the Internet - a distributed system of networks and computers sharing a communications infrastructure. Simply put, no one owns the Internet. More than 90 percent of our Nation's critical infrastructure is operated by the private sector. Our government continues to establish non-intrusive policies that allow our companies to compete while simultaneously helping to protect and prosecute those with cyber criminal intentions.[32] This overwhelming private sector majority gives them voice and influence in the legislative process. However creating a team of private sector partners is fraught with the underlying issues of competition and market distinction. This private-public approach to combat cyber threats requires trust, strong legal protections and shared accountability. There are a number of reasons for the private sector's

reluctance to partner with a cyber coalition and offer full disclosure of their practices, techniques, networks, information, and procedures: proprietary information fuels distinction in a competitive environment; confidentiality agreements between customers and the private sector could erode customer confidence and evade their privacy; legal implications of violating personal information; impact on competition; negative public reaction to any disclosed vulnerabilities; and the possibility of an anti-trust violation. The challenges are exacerbated when dealing with foreign-owned companies or other companies doing business in foreign nations.[33] There is no doubt this topic will be debated for years and arguably without resolution. Cyber criminals are keenly aware of the deficiencies in our collective ability to organize, establish laws and combat cyber terror. Third-party organizations have been suggested as a way to deal with these issues, however the obstacles to success are just as pronounced.

Conclusion

Cyber users at all levels must assess the risk and consequences of joining a Cyber Coalition. As depicted in Figure 1 above, the higher the risk-band the more likely willing-users and seemingly unwilling-users will gravitate to a common cause to combat the cyber threat. Trusting and sharing information to combat cyber terror has a political, economic and social price. Like-minded nations must share in the price of success or the price of failure in cyber space. Through this research I have come to appreciate that a higher risk band will not necessarily drive a state or a non-state player to the seemingly safe haven of the cyber collaboration target zone. Ideology, politics and economics will have a far greater impact on the decision to band like-minded nations into a cyber coalition. James Reed captured my attention by suggesting that the United States itself wants to play by self-interest rules and harshly punish state and/or non-state players that do not support US policy. If other nation-states believe Mr Reed or even a portion of his argument,

the United States is doomed to lose the trust battle. We must learn to trust and share critical e-information and discuss vulnerabilities as we explore new ways to harden our networks, improve our politics, maintain the open flow of commerce, protect intellectual properties and consumers, and establish flexible laws against the cyber villains. It will not be an easy task to balance cyber terror rules without impacting civil liberties, ideology and free market systems. It is likely that non-state actors will continue to be secretly supported by sovereign governments. Academia has a role in researching the balance and consequences between civil liberties, privacy and cyber terror at the national and international level. Use of hegemonic powers will only fuel more cyber social movements to rebel against the United States and our allies. Make no mistake, we have an obligation to protect and defend ourselves and our allies in cyber space. We must use existing first-strike policy to exercise our right to defend ourselves and send a clear message to those that want to do us harm in cyber space.

Several developed nations and certain developing nations could make a significant impact in the success or failure of a Cyber Coalition. However China, Russia, Europe, Iran, Israel, Indonesia, Japan and the United States will likely never see eye-to-eye on any cyber space policy. It is important to note that we cannot seem to agree on a common framework for the term "cyber threat," notwithstanding a draft definition. It is important to employ the necessary safeguards and partnerships within the international community to support and defend the sovereignty of the United States and our e-allies. Coalition building in cyber space is a significant step in the right direction to combat cyber threats.

Endnotes

[1] InternetWorldStats, Internet Usage and World Population Statistics, https://www.internetworldstats.com, (accessed August 20,2011). Internet usage information comes from data published by Nielsen Online, the International Telecommunications Union, by GfK, local Regulators and other reliable sources.

[2] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace", Department of Defense, Washington, DC (2011). Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partners to strengthen collective cyber security.

[3] Colonel Terrence Howard, "The Collaboration Target Zone". The opposing views [willing-transparent and the unwilling-translucent] and Figure 1 [Collaboration Target Zone] were developed by COL Terrence L. Howard. COL Howard is an Army War College Fellow attending the University of Texas at Austin during Academic Year 2011-2012. COL Howard hypothesizes that a cyber coalition must organize among independent communities and non-state players to combat this growing cyber threat. TEAM CyberCo players are motivated by numerous things and events to include self-interest and self-protections. As the network risk vulnerabilities increase [risk bands], COL Howard asserts that willing and unwilling players will normalize and find common ground within the Collaboration Target Zone. He further concludes that US Strategy must focus on the collaboration zone players and engage players outside the target zone. We must attain efficiency and effectiveness in this severely resourced constrain environment.

[4] Howard, Collaboration Target Zone.

[5] Andrew Keen,The Cult of the Amateur: How Today's Internet is killing our Culture, (New York: The Doubleday Publishing Group, 2007), 15.

[6] Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations", Cooperative Cyber Defence Centre of Excellence, (2010): 16-17.

[7]Ministry of Defence Estonia, "Cyber Security Strategy: Cyber Security Strategy Committee", Cyber Strategy for Estonia, Ministry of Defence, (2008): 3-5.

[8] Office of Management and Budget, "Fiscal Year 2010 FISMA Report to Congress", OMB Report to Congress (2010): 12.

[9] Richard Stiennon, Surviving Cyberwar (Lanham, Maryland: Government Institutes, 2010), 151.

[10] Matthew Lynley, "Updated: U.S. defense supplier Lockheed Martin hit by cyber attack", Venture Beat News, http://venturebeat.com/2011/05/28/lockheed-martin-cyber-attack (accessed Februrary 27, 2012).

[11] Will Dunham, "Energy Departmet Discloses Cyber Attacks", Fox News, http://www.foxbusiness.com/technology/2011/10/24/energy-department-discloses-cyber-attacks (accessed February 27, 2012).

[12] Security Technology News Coorespondent, "Harvard University Website Cyber Attack", Security Technology News, http://www.security-technologynews.com/news/harvard-university-website-cyber-attacked.html (accessed February 27, 2012).

[13] Gavriel Queenann, “Israel hospitals come under cyber-attack”, Israel National News, http://www.israelnationalnews.com/News/News.aspx/152104 (accessed February 27, 2012).

[14] Kathleen Hickey, “Hacked foreign government suspect”, Government Computer News, https://gcn.com/articles/2011/06/14/inf-hacked-foreign-government-suspected.aspx (accessed February 29, 2012).

[15] Brain Bottesini, “IA Challenges in an International Environment”, IAnewsletter 12, no. 4 (Fall 2009): 6.

[16] John Rollins and Clay Wilson, “Terrorist Capabilities for Cyberattack: Overview and Policy Issues”, CRS Report to Congress, Foreign Affairs, Defense, and Trade Division, Congressional Research Service, The Library of Congress, (2007): CRS-21.

[17] Wikipedia, ”Conventions on Cybercrime”, http://en.wikipedia.org/wiki/Convention_on_Cybercrime (accessed February 28, 2012).

[18] Booz Allen Hamilton, “Cyber Strategic Inquiry 2008: Enabling Change Through a Strategic Simulation and Megacommunity Concept”, Simulation Lessons Learned CSI'08, Business Executives for National Security, (2008): 4-8.

[19] Wikipedia, “Cyber Shockwave”, http://en.wikipedia.org/wiki/Cyber_ShockWave (accessed March 6, 2012).

[20] Shaun Waterman, “Cyber Storm III aims to protect against the real thing”, The Washington Times, http://www.washingtontimes.com/news/2010/cyber-storm-iii-aims-protect-against-real-thing (accessed February 28, 2012).

[21] Department of Homeland Security, “Nation Cyber Incident Response Plan”, Homeland Security, (2010): 1.

[22] Sarah Gordon and Richard Ford, ”Cyberterrorism Symantec Security Response White Paper”, The Symantic Corporation, http://www.symantec.com/avcenter/reference/cyberterrorism.pdf, (access January 22, 2012): 4-5. It is important to note that there are hundreds of definitions for cyber terrorism to analyze and debate however the study of each definition is beyond the scope of this paper.

[23] Susan Brenner, "At light speed: Attribution and response to cybercrime/terrorism/warfare”, Journal of Criminal Law and Criminology 97, no. 2 (Winter 2007): 382.

[24] Jeffrey Carr, Inside Cyber Warfare Second Edition, (Sabastopol, CA: O'Reilly Media, 2012), 14.

[25] Brenner, 405-406.

[26] Carr, 2-4.

[27] Tom Gjelten, “Stuxnet Raises Blowback' Risk In Cyberwar”, National Public Radio, http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar (accessed March 26, 2012).

[28] Carr, 29.

[29] Andrew Cooper, John English, and Ramesh Thakur, *Enhancing global governance: toward a new governanace.* (Tokyo: United Nations University Press, 2002), 1.

[30] Cooper, *Enhancing global governance: toward a new governanace*, 55-67. The Unite States of America is not, finally, a ‘‘like-minded country’’, nor is it likely to be any time soon; but it contains many like-minded institutions and like-minded people. Under the doleful circumstances of the George W. Bush administration, the need for a ‘‘new diplomacy’’ appears to be more acute than ever.

[31] Cooper, *Enhancing global governance: toward a new governanace*, 268.

[32] Committee on the Judiciary, “Cybersecurity: Innovative solutions to challenging problems”, Congressional Report for the House of Representatives, Washington DC (2011): 1.

[33] Philip Auerswald, Lewis Branscomb, and others, *Seeds of disaster: roots of responsibility*. (Cambridge, New York: Cambridge University Press, 2006), 395-397.