GlobalResearch
Center for Research on Globalization

Understanding Cyber Warfare. From Cyber Warfare to Cyber Resistance

By Rachael M. Rudolph
Theme: Militarization and WMD
Global Research, November 28, 2011
28 November 2011

Instruments of warfare have evolved. Gone are the days of battle-axes, machetes, swords, and men charging in strategic formation or lying in trenches awaiting their foe. Instead, guns, bombs, chemical and biological agents, unmanned aircraft and assault vehicles are used as instruments of war. A more significant change from the past has been the robotic nature of the way conflict is waged, supposedly making more "humane" an inhumane act. The changes witnessed of course parallel technological advances within society, resulting in even more wars and conflicts being waged from behind a computer screen, in a command center, and by remote control. Likewise, the ways in which resistance is carried out will parallel the technological changes and evolving nature of warfare. The rise of cyber warfare and resistance shed light on where we are heading, with both state and non-state actors on almost equal footing in the knowledge of and potential use for viruses, worms and Trojans. Arguably, some actors operating in the realm of cyber resistance are more advanced in knowledge than the states they are battling. Is Cyber Resistance a weapon for checking the traditional and conventional military power of the state? Will it be the key for checking Israel and its inhumane and disproportionate use of force and weaponry against Palestinians?

Emerging Cyber Warfare and Resistance

In 1996, Russian Major Boystov argued that the development of very precise lethal and non-lethal kinds of weaponry to exert pressure over another is necessary today because of the urban concentration of most populations, with electronic weapons being such a direct or indirect means.[1] Discussion of electronic weaponry prior to the 1990s was limited to academic, government and military circles. Rarely were there discussions that entered the public domain. The academic literature cites the US War with Iraq in the 1990s as the point of change.

This point also parallels the rise of Cyber Resistance. Prior to the 1980s, individual hackers were relatively unknown to one another. Well, at least in the context of their geographical boundaries. Chat systems transformed interaction by bringing individuals from all over the world together. They were able to not only interact but also learn from and exchange ideas about the realm of possibility. A common goal united their association and interaction, which was the liberation of information from the shackles of the corporate and governing elite.[2] However, it would not be until the mid-to-late 1990s that cyber collectives would emerge and the early 2000s for the waging of concerted transnational actions that can be considered existing within the paradigm of Cyber Resistance.[3]

In spite of the development of electronic means of warfare and the rise of cyber resistance, states would not publicly admit and/or declare the existence of their cyber warfare programs. In 2007, NATO established the Cooperative Cyber Defense Centre to coordinate and enhance the organization's cyber defense capability. In 2009, the Obama Administration declared America's digital infrastructure to be a strategic national asset; and, one year later USCYBERCOM was established to defend US military networks and to attack other countries' systems.[4] Australia, Britain, Iran, Israel, India, North Korea, and Pakistan are also cited in the literature as being in the process of boosting their cyber war capabilities.

Very few, however, have actually articulated their Cyber Warfare Doctrine.[5] China and Russia are two recognized in the literature as having well-developed theoretical doctrines,[6] while the US has maintained a cloak of silence over its own. The lack of intellectual development in this area, according to Simon Tisdall in his article published in the Guardian in February 2010, is comparable to the period of the 1950s when states were racing to develop their nuclear technological knowledge and programs.

The lack of existing state programs and the uncertainty of engaging in Cyber Warfare led many states to rely on and hire individuals and/or collective groups over the years. For example, Israel hired several individuals to breach the US Department of Defense's computer systems in 1994.[7] India and Pakistan have also relied on an ongoing cyber war between non-state actors from their respective countries. Cyber war is not directed, carried out and waged by these states, but instead by non-state actors that are engaging each other and attacking the opposing government's websites and computers. Use of and reliance on non-state actors by states is likely to change in the years to come as government Cyber Warfare Programs are developed, and as more non-state actors band together to wage in resistance against the growing abuses by those in power.

The Cyber world today remains the realm wherein people can anonymously and legitimately challenge and check states growing abuse of power and infringement on the rights of people, which they are supposed to protect and represent. In the minds of many today and in the media is the global, leaderless collective called Anonymous, where individuals and groups are working independently, interdependently and simultaneously in a framework shaped by and operated according to shared beliefs and interests of those therein participating. There is no centralized structure and each of the entities operating therein has their own independent decision structures and mechanisms for constructing and implementing policies. Anonymous' overall functioning and power lie in the will of people, which is the reason it can and will remain a leaderless movement that encompasses all.

Given everything, it should come as no surprise to many that today states are on equal footing in some cases and have been outpaced in others by non-state actors operating in the realm of Cyber Resistance. The literature on Cyber capabilities ranks non-state actors inside Pakistan as having the potential to rival China and Russia in capabilities and knowledge, which is quite amazing given that these two countries' abilities and existing programs are considered the best. Hezbollah is also ranked high for its cyber warfare program and the ability to carryout cyber attacks. For many of us who write on resistance movements, Hezbollah is considered and respected as one of the best in terms of military capabilities, knowledge and development. Lastly, it should also be noted that some cyber groups specialize in, and are known for, certain cyber activities.

When looking at the concept of and potential for Cyber Resistance, the realm of possibilities

are exciting and seem limitless. Cyber Resistance is here to stay and cyber programs are the future for many existing actors, groups and movements seeking to challenge the existing status quo and engage in conflict with an entity that is stronger in conventional armaments and programs. It is, arguably, the key to finally checking Israel and preventing it from continuing to ethnically cleanse Palestinians from their land. Before addressing this point, a brief examination of what is cyber warfare and the methods it encompasses are necessary.

Attempting to Understand Cyber Warfare

Given the nascent development of Cyber Warfare programs, it is not surprising that there is a lack of consensus on what exactly is meant by the term. Cyber Warfare is considered politically motivated computer attacks on informational, technological and/or physical infrastructures. Some have argued that "war" is not the appropriate reference and is used to evoke a militaristic frame and thus draw a similar response. Proponents of this argument posit that the phenomenon is best captured by acts of sabotage, espionage and subversion. Differences over definition of what constitutes cyber warfare have resulted in a reluctance of many to pursue cyber arms control agreements. The definitional debate will continue to rage for years to come, similar to the debate over defining a terrorist and a freedom fighter. States are likely to continue deeming the challenging non-state actors and/or groups as terrorists, while the people recognize them for what they rightly are, which is resistance.

Cyber attacks, however, are recognized by states as a means for countering an opponent that is superior in conventional and traditional military power. Any informational infrastructure or that which relies thereon can be bugged, hacked, infected, tapped and penetrated. Thus, a multifaceted cyber attack employing various techniques could be highly disruptive to the targeted enemy. The basic notion of and that which most attacks are designed to do go beyond mere annoyance, agitation and irritation to inflict sustained uncertainty, confusion, chaos, and to provoke a feeling bordering on fear. Some attacks also seek to disable or prevent an action. For example, cyber actions to prevent or halt the US government's censoring or blocking of information; its violations of free speech and infringement on the people's human rights; and, using unjust means to put down public unrest. The reasons for attacks are thus political and the cyber means for carrying them out vary.

Types of attacks that fall under the rubric of cyber attacks are evolving, with no clear line or rules for engagement and/or classification of their nature. Hacking, Trojans, worms and/or viruses are the means used for the execution of attacks. Cyber attacks can be categorized into those that are mere psychological or informational in nature and others that are structural. Some of psychological attacks include the giving of or implanting false impressions that masquerade or serve as a decoy for a larger operation; disinformation campaigns that result in errors of judgments; and, web defacements designed to agitate the targeted enemy. While some attacks are carried out for the sole purpose of, geared toward or designed for information collection and cyber reconnaissance, all cyber operations contain this type of attack or strategy.

Some of the structural attacks include the implantation of backdoor, time or logic bombs; changing data or the jamming of systems to produce the dysfunction of the target;

performing data corruption or degradation of computer systems that control monitoring capabilities; development of viruses and the use of denial of service attacks (DoS) to disrupt activity; use of electromagnetic and sound wave technologies to interfere with the frequency and equipment used to operate structures, systems, and weaponry; erasing of hard drives to disrupt development and research; rewriting of software programs to permit remote access; and, tampering and destruction of critical economic and public infrastructure from remote areas.

Cyber attacks can also resemble traditional modes or tactics of resistance such as virtual protests and the shaming or agitation campaigns that utilize social media. Virtual protests and aggressive agitation campaigns have become popular since the start of 2011, with participation significantly increasing. Computerized global campaigns to support the activities on the ground in places like Tunisia, Egypt and Palestine have complimented the traditional modes and tactics of non-violent resistance employed by fellow activists. The collective mobilization of cyber activists and those on the ground has also created a bond that has the potential to transform resistance and the strategies employed in ways not thought possible in the past.

Excitement for new modes, strategies and tactics and the emergence of a paradigm for cyber resistance must be tempered by the fact that carrying out a cyber attack is not easy.[8] Each one requires a significant amount of informational acquisition to identify potential entry points and susceptible points in the communication systems or structure. Afterward, codes must be written and inserted. The first step is sometimes referred to as the "true hack" and the second as the "derivative hack."[9]

A derivative hack does not require a significant amount of computer or programming knowledge for execution, especially not with all the existing software programs available. Regardless, a large cyber resistance attack requires a significant amount of planning, cooperation and participation for its successful execution. Giving the novelty of cyber warfare and the attacks that can be waged, there is very little appreciation or developed methods for assessing the use and success of some of the aforementioned. This is in large part due to the difficulty in knowing the origin of an attack and the length of time between execution and its realization by the opposing side. Of course, some attacks are more readily apparent such as those that recently occurred to disrupt the functioning of the Israel's intelligence and military websites.

Effective or successful attacks or operations are defined as those that intrude upon the enemy's virtual space or network to compromise, degrade, disrupt or impair activity and undermine trust. The disadvantage is that effectiveness can only be measured in minutes whereas conventional weapons can remain effective for years. The upside for many resistance movements and people seeking to check the abuses of the state is that Cyber resistance is more cost-effective than the acquisition of traditional warfare, at least for the time being. Iraqi resistance was able to intercept video feed from the inhumane Assassination Drones for only 30 US dollars.[10] Costs vacillate according to the technological changes in the development of new, or the updating of old, conventional military equipment.

Finally, a person lacking in knowledge of how to hack or to engage in Cyber Resistance can still participate directly or indirectly. This changes, in some ways, the nature of who participates, the quantity of participants, and how some resistance strategies can be waged. The changes have the potential to increase the success or impact some of the

traditional strategies, which have become a bit ineffective over the years.[11] A latent power behind and associated with Cyber Warfare for challenging Israeli policies of genocide and occupation exists, with some attacks having the potential to reduce and/or constrain Israel's use of targeted assassinations. Assassinations are contrary to international law and there is no humane justification for their use. The increased use of them by Israel and the United States sets precedent for how state warfare is likely to change and be engaged in the future, if their abuses are not checked.

Checking Israel with Cyber Resistance?

Cyber war is not a new phenomenon and cyber attacks are familiar in the conflict between Israelis/pro-Israeli and Palestinians/pro-Palestinian activists. Tactics such as web defacements, system penetrations, misinformation campaigns and the use of viruses and Trojans have been used.[12] The year 2000 saw a spike in their use, which garnered some media attention. In addition to web defacements and system break-ins, the Bank of Israel and the Tel Aviv Stock exchange were targeted. The attacks were of course a response to not only Zionist atrocities committed against the Palestinians but also because of Israeli cyber attacks on Palestinian sites, including those of Hezbollah and Hamas. Activists participating in cyber resistance against Israel span the world, but the latter too has its own activists to hit back. Thus, examination and evaluation of past attacks used in this context on both sides, as well as those used by other groups, are necessary to develop better cyber resistance programs, strategies and tactics. It is only through coordination and cooperation in this area that the potential to check Israel becomes a reality.

An examination of the types of cyber attacks carried out elsewhere and in the past provides an understanding of the potential ways Cyber Resistance can be used to check Israeli behavior. Defacement, DoS and cyber attacks for information gathering are already being and have been carried out, but the question begging is whether some of the nuanced attacks and strategies employed elsewhere makes the targeting of drones, domes and electronic censors possible? Given the length of this article, a discussion of domes and electronic censors will be reserved for another day or left to someone else. A brief one will be had, however, on the potential use of cyber resistance for targeting the flying assassinator that kills, maims and injures Palestinians sleeping at night, driving in cars, walking on the streets or attending weddings and funerals. The terrorizing, buzzing noise of the Israeli drone is not limited to Gaza but has also been used to violate Lebanese and Syrian territories to gather intelligence on future targets, whether they are buildings or people.

Israeli UAVs (Unmanned Aerial Vehicles) are used for intelligence, surveillance, reconnaissance and targeting missions. As like most advanced military equipment and the command centers from which they are operated, computer generated technology is the backbone. Drones and other computer-operated equipment can be targeted, especially given previous incidents. Iraqi resistance was able to intercept the feed from US drones, which permitted identification of what was being monitored and removed the element of surprise. In most cases, drones are used for intelligence gathering prior to carrying out an assassination. The feed gathered is sent back to the command center in order to identify potential targets. Iraqi resistance has not alone in its penetration of the drone, however.

According to Sayyed Hassan Nasrallah, Israeli technological control over the

telecommunications in Lebanon has permitted eavesdropping, monitoring of individuals and the collecting information, all of which are used for attacks, assassinations and kidnappings.[13] Israel also has control over the telecommunications infrastructure in Palestine. Before 1997, according to Nasrallah, Hezbollah was able by its technical efforts to monitor an Israeli aircraft that was taking photographs and sending them back to the Zionist Entity. Through electronic penetration, the Islamic Resistance in Lebanon was able to gather some of the films and images captured, which were then analyzed and compared with satellite images by professionals. A lack of expert professionals in the beginning meant that some of the images were not understood, but the introduction and development of Hezbollah's technological capabilities permitted greater understanding. Today, as already noted, the Islamic Resistance Movement in Lebanon has one of the best Cyber Resistance Programs among resistance groups.

Interception of video feeds and the knowledge of the intelligence gathered are not the only way in which cyber resistance can be used. In an incident carried out by unknown individuals, the Creech Air force Base in Nevada was infected with a key logger virus that was not caught until two weeks later.[14] Other means to be used are the jamming viruses and electronic interference. Past attacks using these tactics include jammed or disabled radar systems; and, worms and viruses to target specific functions. All military activities that use computers and satellites for coordination are at risk of equipment disruption; and, all orders and communications can be intercepted or replaced. The realm of possibilities and the strategies to be employed in the realm of Cyber Resistance are limitless and provide a new playground for academics and journalists that write on such matters. Nothing is inconceivable and no shackles can be placed upon ideas generated by the minds of many.

Dr. Rachael M. Rudolph is Head of International Relations for Facilitate Global. She can be reached at rachael.rudolph@facilitateglobal.org.

References

1 Billo, C. and W. Chang (2004). "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," *Institute for Security Technology,* pp. 1-140.

2 Phrack Magazine, "International Scenes," Volume 4, Issue 44.

3 In 1999, individuals in Canada, Norway and Thailand were able to coordinate and cooperate to breach successfully the military computers at Kelly Air Force Base in San Antonio, which is the center for the most sensitive Air Force Intelligence. See: Miklaszewski, J. "Pentagon and hackers in 'cyber war,'" *ZDNet at http://www.zdnet.com/news/pentagon-and-hackers-in-cyberwar/101740 .*

4 Billo and Chang *supra note* 1.

5 Greenemeir, L. (2011). "The Fog of Cyber Warfare: What are the rules of engagement," *Scientific American.*

6 Billo and Chang *supra note* 1.

7 The US Pentagon was hacked again by an Israeli in 1998. See: Thomas, D. (1998). "Sorting Out the Hacks and the Hackers," *A USC Annenberg Online Journalism Review. Http://www.ojr.org/ofr/ethnics/1017969499.php .*

8 Schmitt, E. and T. Shanker (2011). "US Debated Cyberwarfare in Attack Plan on Libya," *New York Times.*

9 Thomas, D. (1998). "Sorting Out the Hacks and the Hackers," *A USC Annenberg Online Journalism Review. Http://www.ojr.org/ofr/ethnics/1017969499.php .*

10 Gorman, S., Y.J. Dreazen and A. Cole, (2009). "Insurgents Hack US Drones," *The Wall Street Journal.*

11 Although there is no standard measure of power or success for the resistance tactics and strategies employed and a quantitative means for ranking resistance movemen7ts, there are common variables used for assessment and evaluation of effectiveness of tactics, strategies and movements.

12 Gentile, C. (2000). "Hacker war wages in Holy Land," *Wired*.

13 See Sayyed Hassan Nasrallah's speech on August 9, 2010, which aired on Press TV. The speech can be found at http://www.youtube.com/watch?v=5odeTwU2zjw.

14 "UAV Drone Virus—What we know so far?" *Cyber Arms.*

Articles by: Rachael M. Rudolph