Cyber power: A state’s element of power?

by Panos Mavropoulos

Introduction

Cyber space, as much as it is difficult to define, is a reality, having intruded in our lives gradually, reaching today a point without return; no one can live without it anymore. Today, a continuously increasing portion of the international human activity is being conducted within or through this expanding notional space.

Lacking an overarching regulatory authority, cyber space’s operation is chaotic resulting in serious issues that need to be dealt with by the states, as the most important actors of the international system. The chaotic operation of cyber space provides the opportunity to various actors, i.e. hackers, crackers, criminal gangs, terrorist groups, hacktivists, states or even groups of states, to resort to illegal activities, each one with its own aims and objectives. Illegal activities in cyber space constitute a serious threat, which no state is immune from. Governments and private companies’ systems have been under attack through cyber space for many years now. Well planned cyber attacks can disrupt public services and interfere with the production and delivery of essential goods and services thus becoming a threat to a state’s national security.

Strategy in the age of cyber space

When cyber power presented serious evidence as a new and “important domain in interstate conflict”[i] ideas started developing, related to preventing or defending against cyber attacks and even mounting organized cyber attacks within or through cyber space against other states. Seen from this point of view, “cyber power has posed a challenge for strategists since its advent, and the questions have only grown more pressing with the revelation of the Stuxnet malware attacks on Iranian nuclear sites” [ii].

The development of cyber power of course is not an exclusive privilege of states; it is shared with a wide variety of actors that co-exist in cyber space. Cyber power thus acquired is currently used by those actors to conduct any sort of illegal activities in cyber space, which can be distinguished in two broad categories; those that fall under the authority of the law enforcement agencies and those that belong to the realm of national security. The term prevailed for the description of state sponsored activities in cyber space, mostly against other states, is *cyber war*. We should be careful though with the use of the term. So far “state-to-state computer network attacks there have not been; espionage, yes, of course; irritating hacktivism, certainly; but cyber war, no, at least not by a careful definition”[iii].

There are many interesting issues associated with the conduct of cyber war, the majority of which belong to the tactical - technical level. This level of cyber talk dominated international literature (and in fact still does) since the appearance of the term *cyber*; public discourse almost ignored discussion of cyber power beyond this level. With the exception of very few papers, the use of cyber power to achieve political ends, which is the realm of strategy, has been the object of books and articles only recently or to put it in Colin Gray's words; "High-quality strategic theory about cyber simply is not there in the literature during the 1990s and most of the 2000s[iv]".

This is not the essence of cyber war though; cyber power is used against other state or non-state actors in pursue of a wide variety of ends, which in strategic theory parlance are called *political ends*. The real issue therefore we need to ask ourselves and, ultimately, answer, is the purpose for which we should raise and use cyber power; in other words, what is the political aim cyber power will be employed for. Because, no matter how good we become in using cyber power, it is all irrelevant if we have not chosen a clear-cut political end to be pursued, suited to the particular characteristics of cyber power, a concept expressed two centuries ago, albeit for military power, by the great Prussian General, theorist and philosopher of war, Carl von Clausewitz, in his monumental work *On War*. Therefore, as it applies to the overarching concept of war in general, cyber war is not an end in itself but it is rather conducted for the purpose of achieving political ends.

Almost all strategists and cyber power experts alike tend to equate cyber power with military power or, even worst, to consider it subordinate to military power[v]. This in its turn means that cyber power, when considered in the context of a crisis or actual war, should play a supporting role to that of military operations. That may be so in some, rather limited, cases but this consideration underestimates cyber power, its dynamics and prospects. Cyber power differs from military power in the sense that it cannot kill directly and cannot occupy territories[vi]; but the same applies to the other state's elements of power. If war is seen as an effort to impose one's own will on that of the enemy[vii], then cyber power can be considered as a means to that end (with other means being diplomacy, information, military, economy (DIME)), an autonomous element of power, with its own special characteristics and capabilities. Following a slow start in a supporting role to the other elements of power, cyber power took its own life and reached today a point where it can seek to achieve, as a primary element of power, political ends, with the other elements of power in supporting roles. As cyber space expands quickly to include progressively larger portions of human activity and at the same time cyber capabilities evolve, those political ends will expand to include more ambitious ones.

If war is the realm of politics and political leadership, and warfare is the realm of military and its leadership, then the question raised is in whose realm cyber war falls in? Should we accept that cyber power is a means at the state's disposal to manage a crisis and therefore can be characterized as one of the state's elements of power, we should also accept that its use for the attainment of political ends is planned and conducted at grand strategy level.

Lacking the essential elements of causing harm and damage, as argued by the majority of experts, for coercing potential enemies, the next question naturally raised is how an actor, using its cyber power, can influence the political behavior of a potential enemy. In other words, where cyber attacks should be directed, what the cyber objective would be and what the center of gravity of the potential enemy would be for the cyber war effort to be directed against.

Submission to the opponent's will is obviously decided by the respective government, following a cost-benefit analysis and taking into account many factors. One of these factors is the will of the people. Therefore, in planning our strategy "to compel our enemy to do our will"[viii], one of the options is to erode the will of his people, which in its turn can be done in many different ways. The North Vietnamese tried it successfully during the Vietnam War by resorting to a protracted war, which finally eroded the American people's will to support the case[ix]. This strategy is not new at all though. Italian Air Force Major General Giulio Douhet, the first air power theorist, in his book published in 1921[x], highlighted the moral effects of aerial attacks which could "… be directed … against objectives of least moral resistance"[xi], referencing as targets "peacetime industrial and commercial establishments; important buildings, private and public; transportation arteries and centers; and certain designated areas of civilian population as well"[xii]. Attacking those targets one can inflict pain and fear among the civilian population and ultimately erode its will to support the war.

While the opponent's center of gravity for our cyber war effort to be directed against is the will of the people and indirectly, the government, which is ultimately responsible to make the decision of yielding to the opponent's will, the erosion of the opponent people's will can be achieved by creating chaos in the country and undermining the confidence of the people in its government vis-à-vis its capability to provide basic services. This in turn can be achieved by attacking the information technology infrastructure. The standardization of components required in the information technology industry, which is done primarily for economical reasons, exposes those systems to cyber threats. No system with information technology infrastructure is excluded, no matter if it is connected to the Internet or not.

An important subset of the information technology infrastructure is a state's critical infrastructure, which is defined as the infrastructure vital to "the defense and economic security [of the state], the smooth functioning of government at all levels, and society as a whole"[xiii]. Generally, the critical infrastructure includes banking and finance, emergency services, energy production and distribution systems, communication networks and services, transportation, water and food production and supply systems, etc. Attacks on national critical infrastructure have been going on for years now. Nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their systems[xiv]. National critical infrastructure will be a priority target on which the enemy's cyber attacks will be directed, provided they are, in some way, accessible. Organized cyber attacks against critical infrastructures can not only cause substantial economic costs on the intended target country, but they can also cause chaos in the functioning of the state, while at the same time can cause, indirectly, harm and damage, bringing everyday life almost to a halt, thus undermining the people's will and its confidence to its government.

Case study: The Stuxnet worm

Looking back at cyber war's short history while Russia-Georgia short war in August 2008 showed cyber power's supporting role to that of the military, cyber attacks against Estonia in April/May 2007, and even better the Stuxnet cyber incident against Iran proved that cyber power has already reached the point of an early maturity. The Estonia case proved that cyber war against a nation-state, under certain conditions, in not a myth but it is real, here and now. The Stuxnet case, on the other hand, is an indication of the improvement of cyber capabilities, the higher ambition of political ends being able to be pursued and achieved through cyber war and the autonomy achieved by cyber power vis-à-vis the other elements of power. The Stuxnet case, the first peacetime act of cyber war[xv], is illustrative; we will use it to test the validity of our thoughts expressed above.

Though not explicitly declared, the political aim pursued in the case of Iran's nuclear program by most of the international actors was the cancelation of her nuclear program. The available means for dealing with the problem were the elements of power, namely diplomacy, economy and military power, with information in a clearly supporting role.

Options that could be implemented for the achievement of the aforementioned political aim consist of various combinations of the available means, each one with its own associated risk. Each of the options uses a primary element of power with the rest in supporting roles. The available options include (but are not restricted to) coercive diplomacy, economic sanctions, military power (in the form of bombardment, air strikes, use of Special Forces or even invasion of Iran) and cyber attacks.

The international community up to now has used diplomatic and economic means; supported by the threat of use of force. Diplomacy as a primary means has obviously failed to produce the desired outcome and ultimately achieve the desired political end. Having failed to convince the Iranians to stop their nuclear program, the international community escalated with economic sanctions in an attempt to coerce and compel them to do its will, while at the same time continued the diplomatic efforts. The sanctions have been going on for some years now without desired results. All this time, the military option was never off the table for the obvious reason to work in support of the other options.

Escalation with the use of military power in the form of one or a series of raids or even an invasion of the country is an option expensive in both, diplomatic and economic terms.

Before resorting to the use of military power though, it was decided to use cyber power in the form of the Stuxnet worm. "Estimates suggest that Stuxnet set Iran's nuclear program back by several years"[xvi] and this was as much as Stuxnet could achieve, given all its current capabilities and limitations. As a side effect, which shouldn't be overlooked, "Stuxnet must have had significant implications for Iranian morale as well due to the uncertainty surrounding the attack"[xvii]. The use of cyber power proved to be a credible alternative option, cheaper and, more importantly, effective. Its use bought for the international community time, either for the sanctions to be given more time to work or for the military option to be better prepared, while at the same time showed the Iranians that escalation is a way forward, and at the end of that trail is the use of military power.

The Stuxnet operation was planned and executed at “state” (actually ad hoc alliance) level and had nothing to do with the application of military power. Therefore, cyber power was used at the level of the other elements of power, as a peer equivalent of diplomacy, economy and military power. Its effectiveness cannot be compared to that of military force, but the same applies to its cost, be it economic or human, and the impression to the rest of the world.

If grand strategy is the orchestration of all available elements of power for the achievement of a chosen political end, then we are in the middle of a full blown grand strategy with the use of all available elements of power, with primacy shifting progressively from diplomacy, to economy, to cyber power and, as last resort, to military power in pursue of the political end of cancelling or at least delaying Iran’s nuclear program. Among the elements of power, cyber power stands out as a cheap, easy to implement and rather effective means.

Lukas Milevski, although he sees the Stuxnet attack as “an instrument of strategy and policy”, argues that it “may be judged a tactical success but a strategic failure” [xviii]. In order for the attack to be called strategic success or failure, it should be judged against the political end for the achievement of which it was employed. Obviously it was judged that cyber power by itself was, for many reasons, insufficient to affect the Iranian political will to continue its nuclear program. Therefore, in this case, cyber power was used in concert with the other available elements of power with the purpose to delay (instead of abandon) the nuclear program, by causing physical damage to the nuclear facility. If this true (as it seems most likely), then the attack was a strategic success; if on the other hand the aim was to coerce the Iranians to give up their nuclear program for good, then it was a typical strategic failure of not matching “available means” to desired “ends”. But this would be such an ambitious objective to be pursued; cyber power, with all its capabilities and the myth surrounding it, can achieve only so much. The strategic objective should not ignore the capabilities and limitations of the available means and should be adjusted accordingly. What Colin Gray reports for “military” applies also to “cyber”; “The military means of war are, of course, vital, and they must be allowed to influence—even ‘radically change’—the political aim.”[xix]

Epilogue

We cannot agree more with David Betz’s argument that “cyber war is not coming”[xx], albeit with a different meaning; cyber war has already arrived; it is here and now!

While there is truth in Danny Steed’s statement that “[t]here has simply not been enough experience of actors utilizing Cyber means to attain political ends …”[xxi], and in Martin Libicki’s similar one that “[t]here are reasons to doubt that cyber war has what it takes to coerce a state. No one has yet died in a cyber attack.”[xxii], two years after Steed’s paper and four years after Libicki’s book the cyber landscape looks very different; while coercion is obviously not the strong point of cyber power for the time being, cyber capabilities continue evolving. It won’t be long before cyber power will be able to cause large scale harm and destruction, even as a second order effect. There is already enough evidence that cyber power has reached a maturity stage to be used for the attainment of (limited) political ends, making it thus a peer equivalent of the other elements of power of a state, namely diplomacy, information, military and economy. The political ends might not be glorious as those attained through military power, but at least they fit well to its particular characteristics. Today, cyber power has the potential to be used as a means to inflict pain and fear onto the opponent's people and erode its will to the point where it will exert pressure to its government for submission to the attacker's will.

On the other hand, those capabilities, combined with the existing level of communication and information infrastructure of most state or non-state potential opponents, are not adequate to wage standalone cyber war, except in limited scale and even then always combined with the threat of use of kinetic force.

[i] Will Goodman. "Cyber Deterrence: Tougher in Theory than in Practice?" (Carlisle: Strategic Studies Quarterly, Fall 2010), 103.

[ii] Lukas Milevski. "A special operation in cyberspace". Joint Forces Quarterly 63:4 (4th quarter 2011), pp. 64-69.

[iii] Colin S Gray. "Making strategic sense of cyber power: Why the sky is not falling?" (Carlisle: Strategic Studies Institute 2013) & Joseph S. Nye. "Cyber Power". (Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010).

[iv] Gray, "Making strategic sense of cyber power: Why the sky is not falling?", 7.

[v] Martin C. Libicki. "Cyberdeterrence and cyberwar". (Santa Monica, CA, USA: RAND Corporation 2009).

[vi] Danny Steed. "Cyber Power and Strategy: So What?". Infinity Journal, 2. (Spring 2011), pp. 21–24; Libicki, "Cyberdeterrence and cyberwar".

[vii] Carl von Clausewitz. "On War". Michael Howard and Peter Paret, eds. and trans. (Princeton: Princeton UP 1976).

[viii] Carl von Clausewitz. "On War", 75.

[ix] Harry Summers. "On strategy: a critical analysis of the Vietnam War". (New York: The Random House Publishing Group 1982).

[x] Giulio Douhet, "The Command of the air". (Washington, DC: Office of Air Force History 1991).

[xi] Douhet, "The Command of the air", 22.

[xii] Douhet, "The Command of the air", 20.

[xiii] John Moteff & Paul Parfomak. "Critical Infrastructure and Key Assets: Definition and Identification". (Congressional Research Service, The Library of Congress, October 1, 2004).

[xiv] McAfee, "Critical infrastructure protection report", March 2011.

[xv] Milevski. "A special operation in cyberspace", 64.

[xvi] Milevski. "A special operation in cyberspace".

[xvii] Milevski. "A special operation in cyberspace", 65.

[xviii] Milevski. "A special operation in cyberspace".

[xix] Gray, "Making strategic sense of cyber power: Why the sky is not falling?", 30.

[xx] David Betz. "Cyber war is not coming". Infinity Journal, 3, (Summer 2011), pp. 21–24.

[xxi] Betz. "Cyber war is not coming", 23.

[xxii] Libicki, "Cyberdeterrence and cyberwar", 124.

To cite this article: Mavropoulos Panos, *Cyber Power: A state's element of power, 21 October 2016, http://www.warandstrategy.gr.*