TURKEY'S FUTURE CYBER DEFENSE LANDSCAPE

Asst. Prof. Can Kasapoğlu

Research Fellow – EDAM

1. Introduction

Turkey's internet usage is rapidly growing through social media enhancements, private sectors utilization, and state-owned enterprise networks. Growing interconnectedness, Turkish critical national infrastructure's dependence on networks, and cyber attacks have introduced the complex realities of cyber security to the Turkish national security agenda. In this context, Ankara initiated the first legal framework for national cyber security coordination, The Decree on Execution and Coordination of National Cyber Security Affairs (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar), on October 20, 2012.[1] Furthermore, the "National Action Plan for Cyber Security" was adopted in 2013. The Action Plan underlined the hardships of detecting cyber attacks and placed special emphasis on the protection of critical national infrastructure and sensitive information.[2] In tandem, the Turkish administration launched the first inter-agency-level cyber drills in 2011, and a cyber command was established within the Turkish Armed Forces.[3]

Despite these efforts, cyber threats have been growing more swiftly than Turkish countermeasures. As a NATO member state, Ankara has to both ensure its own cyber security and contribute to the alliance's cyber defense. In doing so, both Turkey and NATO allies will need to develop a crystal clear understanding of cyber warfare, both in offensive and defensive terms.

It should be mentioned that even a purely policy-oriented study on cyber warfare requires vigorous theoretical conceptualization across military and security domains. For a comprehensive analysis of Western cyber security doctrines and concepts suggests that Turkey has a long way to go in perfecting the standardization of its threat calculus emanating from hostile cyber activity. Second, cyber warfare resembles air power discussions debating whether or not practice was derived from theory through creative conceptualization. In this regard, a 2002 study from the Center for Strategic and International Studies (CSIS) draws attention to a comparative assessment between cyber terrorism and the World War II air power theory and application:

> "Cyber-terrorism is not the first time a new technology has been seized upon as creating a strategic vulnerability. While the match between theories of cyber-warfare and air power is not precise, a comparison of the two is useful. In reaction to the First World War, European strategists like Douhet and Trenchard argued that aerial bombing attacks against critical infrastructure well behind the front lines would disrupt and cripple an enemies' capacity to wage war. Their theories were put to the test by the U.S. Army and Royal Air Forces during World War II in strategic bombing campaigns aimed at destroying electrical power, transportation and manufacturing facilities. Much of the first tranche of literature on cyber attacks resembles in many ways (and owes an unspoken debt to) the early literature on strategic bombing."[4]

In order to develop a good understanding of Turkey's vulnerabilities in confronting possible cyber attacks, one should first contextually explain the correlation between emerging technological trends and threat perceptions and how they shape future warfare. The following section will first shed light on the effect of cyber capabilities on warfare as the next Revolution in Military Affairs (RMA). It will then lay out current and potential hostile cyber trends and the state capabilities that Turkey and NATO should consider. The third section will explain cyber space as the fifth domain of fighting wars with a special focus on network-centric warfare. The fourth section will focus on non-state threats and provide a net assessment for Turkey. Finally, the study will present its conclusions and policy recommendations.

2. Conceptualizing the "Cyber-Blitz": Cyber Warfare as the Next RMA

Built on Soviet Military Chief Nikolai Ogarkov's concept of "military technological revolution," Revolution in Military Affairs (RMA) connotes more than mere technological shifts. RMA can be described as a decisive breakthrough in combat-effectiveness due to drastic changes in technology, strategic culture, organization, doctrine, training, strategy, and tactics. It is the application of technology into military systems combined with innovative concepts and organizational adaptation.[5] In Andrew Krepinevich's famous work on RMA titled "From Cavalry to Computer," he draws attention to computer-assisted design and manufacturing effects in advanced simulations, thereby, enhancing military organizations' abilities.[6]

Within this framework, it could be argued that cyber warfare should be considered as the next – or the current – Revolution in Military Affairs. In this regard, operating advanced battle networks to detect, identify, and track targets and managing intelligence-surveillance-reconnaissance (ISR) systems necessitate access to orbital and cyber dimensions of the global commons. As a result, the cyber arms race has already brought these dimensions to the forefront through counter-network attacks, anti-satellite systems, and directed-energy weapons systems. In fact, competition in space and cyber space domains, which advanced arms such as smart munitions depend on, would have direct and significant consequences on battlespace management, command & control (C2), and target acquisition with regard to information flow about real time and space[7].

Related but not limited to cyber warfare, cyber espionage is also an emerging field in which cyber-technological developments are translated into security tools. Cyber-technological breakthroughs made spying possible without leaving one's home country, and in return forced nations to run counter-espionage activities in the cyber domain. Furthermore, a new "non-profit" cyber espionage sector has already become efficient through public release of sensitive information[8].

One should avoid rigid distinctions between cyber functions when considering future warfare scenarios and strategic forecasting. In fact, cyber warfare blurs the "civilian-military divide." The product of decades of innovation and experimentation, cyber weapons and robotics will constitute the main pillars of the next RMA. These are all technology-intensive assets that are products of decades-long innovation and experimentation[9].

In order to develop an historical and policy-oriented context on cyber warfare, continuing to use military history to explain the effects of information superiority on the battlefield is key.

Without a doubt, new war-fighting capabilities have always brought critical superiorities as well as critical vulnerabilities. For example, Hannibal's war elephants were the heaviest and most formidable asset on the battlefield. However, at the Battle of Zama, Scipio Africanus's javelin units, the velites, blinded the elephants from close range, turning the war elephants into a threat to following friendly units rather than a reliable heavy vanguard.[10] The same could be said for the information and computer networks of modern armies. As modern armies enjoy better advantages in information superiority thanks to computer networks and advanced network infrastructures, these advantages also create opportunities for opponents to exploit "new attack surfaces."[11] Neither the Turkish Armed Forces nor NATO are exceptions.

From a military standpoint, it would be fair to argue that cyber warfare depends on information superiority and control over the battlespace. John Arquilla and David Ronfeldt analyzed the Mongolian hordes of the 13th century to conceptualize cyber warfare. According to the authors, although the Mongolians were frequently outnumbered, Mongolians' light and swift cavalry enabled the generals of the steppes to utilize information superiority through systematic command & communications.[12] Resembling the Mongolians' success in translating information superiority into combat capabilities, cyber war, as described by Arquilla and Ronfeldt, is "…conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first."[13]

Although much has been built on Arquilla and Ronfeldt's work their quote from Carl von Clausewitz at the beginning of the study depicts cyber warfare's transformational effects on war: "…knowledge must become capability."[14] They underline that having the best information about the battlefield is as crucial as putting more labor, technology, and capital in the battlefield.[15]

2.1. Tangibility and Visibility in the Next RMA

Cyber warfare entails not only a technological breakthrough but also a set of drastic improvements in organization, doctrine, concept, and military thought. American cyber defense spending hit a historic peak of $4.7 billion USD in President Obama's 2014 budget with an increase of some $800 million.[16] Comparatively, Washington's 2014 cyber defense budget was larger than what Denmark, Finland, or Jordan spent on overall defense in 2013.[17]

Re-organization within the U.S. Army accompanied the budgetary shift. In 2009, then U.S. Secretary of Defense Robert Gates directed the U.S. Strategic Command to establish Cyber Command (USCYBERCOM), which achieved initial operational capability on May 21, 2010.[18] The new command's mission statement indicates that USCYBERCOM "plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyber space operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyber space and deny the same to our adversaries."[19]

Similarly, the Israeli Chief of Staff Gadi Eizenkot decided to establish a branch within the Israeli Defense Forces (IDF) that would consolidate all the nation's cyber capabilities.[20] The news of the creation of Israeli Cyber Command surfaced around the same time as Defense Minister Moshe Ya'alon's public confirmation that Israel had been targeted by Iranian cyber attacks during the 2014 Gaza War, albeit with no significant damage.[21]

Russia, the usual suspect behind cyber operations against Estonia, Georgia, and Ukraine, is another country expanding its cyber capabilities. Moscow approaches cyber operations as part of its foreign policy and hybrid warfare strategies.[22] Seeing as how cyber offense played a battering ram role in the Russian aggression in Ukraine, it seems that offensive cyber operations have already been integrated into Moscow's military thought and even doctrine. In order to counter the cyber threat posed by Russia, NATO established the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, in 2008. The Center's mission is to "enhance the capability, cooperation, and information sharing among NATO, its member nations, and partners in cyber defense…"[23] Furthermore, following the 2014 Wales Summit, NATO put more emphasis on cyber defense and security by endorsing a policy that confirmed cyber defense as a core task of collective defense.[24]

China can also be regarded as a rising power in cyber space. Chinese cyber warfare programs are more centered on fostering offensive capabilities compared to other players in the cyber domain. There are even analyses stating that modern Chinese cyber capabilities improved upon the KGB's industrial espionage methods and pose the gravest threat to U.S. technological superiority.[25] In terms of China's cyber doctrinal order of battle, it is believed that Unit 61398, a special cyber team under the Chinese General Staff's 3rd Department, is responsible for overseeing "computer network operations." China Telecom is reported to have provided special fiber optic communications for the unit, and the unit's personnel size is estimated to be between hundreds to thousands of soldiers.[26] The Chinese General Staff directly answers to the Communist Party's Central Military Commission. Thus, Unit 61398's cyber activities are subject to the highest level of political oversight and the highly centralized decision-making system under communist China.

Unit 61398's cyber activities can arguably be classified as an Advanced Persistent Threat (APT). APT "represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms."[27] APT's are one of the most important emerging threats as potential adversaries seek to harvest sensitive information using this method, targeting both industry and government.[28]

From a broader perspective, it would be fair to say that the People's Liberation Army's (PLA) warfighting concepts are evolving into the systematic incorporation of cyber warfare, signal intelligence, anti-satellite capabilities, psychological warfare, and information operations. The PLA's military geopolitical reading extends to battlespaces that are created by the electromagnetic spectrum, cyber space, and space, all of which culminates in a final "virtual battlespace."[29] In practice, such an approach would introduce a Chinese version of joint warfare and combined arms operations that includes electronic warfare, precision strike, and cyber warfare. Building on the Soviet concept of radio electronic combat (REC) during the Cold War, Chinese military strategists assess that by expanding the limited Soviet REC approach, which was only applied to limited battlespace or limited tactical situations, the PLA could elevate the REC approach to the strategic level. The key element of this approach is the integration of space and cyber space.[30]

Last but not least, the Iranians enter the picture as an emerging actor with high ambitions in cyber space. Like many other authoritarian regimes, Iranian cyber efforts initially focused on internal security. Following the 2009 protests, Tehran installed a sophisticated, Chinese-built surveillance system to monitor all communication within the country.[31] After experiencing the disruptive effects of cyber technology following Stuxnet, Supreme Leader Ayatollah Ali Khamenei authorized the establishment of a new Supreme Council of Cyber space in 2011 with a focus on both defensive and offensive duties. The Council consists of several intelligence and security branches as well as the ministries of culture and communications. The Islamic Revolutionary Guards Corps (IRGC) plays an important role in the Iranian cyber security apparatus. Moreover, Iran held its first cyber drill in 2012 and increased its cyber operations budget by $20 million since President Rouhani assumed office.[32]

Following Stuxnet's relative success in ruining about 20% of the nation's nuclear capabilities, Tehran began to more heavily invest in an assertive program to train "cyber warriors."[33] Within this program and among these cyber warriors, "there is quite a substantial hacking community within Iran. The skills of these hackers range from unskilled amateurs that can use software tools that are developed to exploit already known vulnerabilities to skilled hackers that find new vulnerabilities and exploitations."[34] The featured members of the Iranian hacking community are Iran Babol Hackers Security Team, Ashiyane Digital Security Team, and Iran Hackers Sabotage Team.[35] Reported Iranian cyber attacks on Saudi Aramco and the Qatari RasGas showed the magnitude of Iranian cyber offensive capabilities in regards to sensitive energy assets in the Gulf region. Similarly, during the cyber attacks on the two key Gulf Arab energy firms, some American banks were also targeted by denial of service attacks.[36]

In light of this overview, it could be argued that Turkey and NATO will face more menacing cyber challenges in the 21st century. Apart from a state actor's cyber warfare capabilities, all the aforementioned capabilities could be translated into cyber proxy war threats within emerging security challenges. State actors could opt for launching false flag operations, use hackers, as well as third state parties. Such a complex threat landscape poses threats to Turkish national security as well as NATO cooperative security and collective defense. Along with actor-based assessments, cyber efforts should focus on cyber warfare as the fifth domain of war and how its effects are translated into a network-centric warfare environment, enabling Turkish and NATO allies to better understand the cyber threat calculus.

3. Conceptualizing the Fifth Domain of War: Cyber space and Network-Centric Warfare

The information systems environment that will form the cyber battlespace consists of three layers: physical, synaptic, and semantic. Cyber offensive capabilities and support operations for network-centric operations will operate in this three-layered landscape. The physical layer refers to hardware, computers, cables, and routers with circulation varying from radio frequency to energy to electrical signals and photons.[37]

This layer is vulnerable to kinetic military actions, especially given the current trends in precision-guided munitions (PGM), deep strike options, Special Forces operations, and stealth capabilities. The syntactic layer refers to the orders that instruct information systems with tasks that circulate through the physical system.[38] This layer is and will remain vulnerable to hostile hacker activity, and defensive cyber capabilities will be needed to protect information systems. Finally, "the semantic layer provides meaning to the information content," thus making it vulnerable to deceptive activities.[39] In this respect, it should be underlined that contemporary military parameters are harbingers of "non-obvious wars" in which "identity of the warring side and even the very fact of warfare are completely ambiguous" due to technological and organizational shifts.[40] Thus, this paper utilizes such a paradigm to categorize cyber warfare's role in future network-centric operations.

Cyber warfare's battlespace categorization aids decision makers in formulating future cyber warfare operations and topography. Although cyber space is perceived as a new domain of war, the physical layer of the information systems environment still necessitate the involvement of traditional land, naval, air, and space assets.. Furthermore, cyber operations in synaptic and semantic layers are tightly connected as hostile hacker activity might couple with non-kinetic and deceptive psychological operations. Hence a new form of "combined operations" in cyber space, which would simultaneously take place in the physical, syntactic, and semantic layers, could drastically alter the scope of offensive and defensive cyber operations.

Apart from its multi-layered landscape and topography given hitherto, perceiving cyber space as the fifth and new domain of war does not necessarily mean that such a categorization will isolate cyber space from other domains of war. On the contrary, this study anticipates that cyber space and cyber warfare will most probably play essential roles in future network-centric operations. As indicated in a 2012 study by Liles et al., applying military principles to cyber warfare means the

> "…layering of the digital information technology environment upon the weapons platforms of the Army. This gives the nation-state a significant information edge over the adversary. Layering cyber space capabilities onto terrestrial weapons platforms is not functionally different from using naval forces to support land forces. Another example might be space assets, such as reconnaissance satellites, that support all natural domains (air, land, sea) similar to how cyber supports command and control."[41]

The rise of network-centric warfare will give cyber assets a great advantage in terms of operational and tactical capabilities. The successful outcome of network-centric operations and warfare depends on information superiority over the adversary through generating combat power by effectively linking actors, sensors, and decision-makers.[42] From a military standpoint, such an approach drastically alters the correlation between time, battlespace, and deployed forces. In other words, thanks to network-centric operations, widely dispersed forces can now be used in expanded battlespaces and enjoy improved communications and synchronization.[43]

Finally, it should be underlined that the antithesis of network-centric warfare, not only in terms of military technology but also military thought, is a platform-centric approach. Colonel Alvin Bailey from the U.S. Army formulates key limitations of platform centric warfare as follows:

> "The US Army has the most feared, sophisticated, and lethal armored vehicles in the world. The Abrams Tank and Bradley Fighting Vehicle moving at high rates of speed across the desert, brings fear to the US adversaries. The implementation of these platforms have been so successful, the enemies do not get themselves into a position where they are forced to engage US armored vehicles in the open desert. Although the Army has successfully used Platform Centric Warfare for many years, there are several problems with relying on them in future military operations. It is difficult to rapidly deploy these traditionally large platforms. The US Army has not successfully automated the platform utilizing modern technology across the entire force. Stovepiping of information presents information sharing between systems. Finally, bandwidth constraints have limited information sharing using existing technologies. The aforementioned key issues will be examined as they reveal limitations in the current Platform Centric Warfare approach and the need to pursue an alternative conceptual framework."[44]

Therefore, unless Turkey and its allies develop adequate offensive and defensive cyber capabilities, Turkey's network-centric concepts can be inevitably rendered abortive in future battlegrounds and reduced to "accidental platform-centric" concepts.

4. Cyber Weapons as Strategic Weapons: Rethinking a Capabilities-Based Model for Turkish and NATO Cyber Security

Another debate on cyber weapons is centered on whether or not they can be categorized as strategic weapons. It is vital to understand the nature and characteristics of the weapons systems to assess the threat perceptions for Turkey and its allies. The complex characteristics of strategic weapons include catastrophic destructive capabilities, psychological terror-weapon effects, and assured destruction.

According to Tabansky, the right way to conceptualize cyber warfare should be akin to the approach to any new weapon system. Analysts should work with familiar variables such as range, extent of destruction, and cost and political limitations of use.[45] Additionally, the first-strike advantage is fairly clear in cyber warfare. In this regard, the benefits of cyber technology in targeting command & control structures make attack more appealing than defense, thereby, curbing the adversary's retaliation capacity.[46] The availability of a broad target set, such as critical national infrastructure, the banking and finance system, sensitive communications, and Internet use, also makes cyber weapons even more menacing than conventional arms.

In tandem with the proposed methodology above, a Center for Strategic and Budgetary Assessments (CSBA) report considers a similar way to judge cyber weapons and cyber warfare:

> "One important quality that both nuclear and cyber weapons share is that the competition favors the offense. Put another way, given equal resources, the side that invests in offense has the advantage. With respect to the nuclear competition, the U.S. military, generally acknowledged to be the world's most technically sophisticated, has yet to develop an effective defense against nuclear ballistic missile attack despite over a half century of effort and hundreds of billions of dollars. Similarly, it appears that it is far less taxing to develop an offensive cyber capability than it is to defend against the various forms of cyber intrusion and attack. Were the case otherwise, cyber economic warfare, cyber crime, and cyber espionage would not be the problems they are."[47]

However, one cannot yet categorize cyber weapons as "perfect strategic weapon systems." If so, how can we categorize these emerging military and weaponized assets? A 2012 Royal United Services Institute (RUSI) study argues that high-potential cyber weapons can be compared to "anti-radiation missiles" that are "fire-and-forget" weapon systems, which require specific target intelligence to be programmed into the asset.[48] From a technical perspective, advanced anti-radiation missiles are designed to destroy integrated enemy air defense by employing emitter geo-location, active terminal guidance, and network integrated communications.[49] In military planning, anti-radiation missiles are mostly used in SEAD (suppression of enemy air defenses) missions to pave the ground for larger follow-up air strikes.

On the one end of the spectrum, cyber weapons are mostly malicious software, known as malware, that are able to influence systems but incapable of efficiently penetrating them for inflicting serious harm. The "high-potential end" of the spectrum refers to the malware that are capable of penetrating protected systems to inflict serious damage through autonomous hostile conduct.[50] Thus, as the potential for cyber weapons' ability to paralyze an adversary, right before an engagement, rises, the anti-radiation missile analogy becomes more appropriate.

Without a doubt, cyber warfare enables belligerents to strike strategic and tactical targets remotely, while minimizing operational risks during a campaign. This advantage depends on the ambiguity of a cyber attack, which forces the victim to distinguish between an attack and a technical glitch, whilst rendering it difficult to connect an event with a result.[51]

From a military intelligence perspective, cyber's detection and identification of strikes shows similarities to those of biological warfare. At the outset of a cyber attack, the utmost priority is given to efficiently detecting and identifying the hostile activity and to take the necessary countermeasures.[52] Like biological weapons programs, cyber weapons programs are easy to hide and offensive capabilities can be fostered through dual-use technological improvements. As initial detectability varies by bio-agent, the same principle can be used to judge cyber-agents. Due to the involvement of private sector and individual contractors, identifying belligerents is highly demanding in the cyber warfare battleground.

As a result, like biological weapons nonproliferation measures, cyber weapons and cyber warfare necessitates advanced military intelligence capabilities to monitor state and non-state actors at the same time. The intelligence requirements in both biological warfare and cyber warfare should deal with a broad spectrum of capabilities and intentions, which have to cover commercially available tools for individuals, small extremist groups, and even lone-wolf aggressors.

5. Non-State Threat Assessment for Turkey: A Volatile Cyber Security Environment

As states in the Middle East are in decline in a Weberian sense, non-state violent groups show significant interest in cyber operations, leading to the spillover of conflict into cyber space. In this regard, the Syrian Electronic Army (SEA) deserves attention. The cyber operations group's main core is located in Dubai with other members in Syria. Funded by Bashar Assad's cousin Rami Makhlouf, The SEA is called "a real army in virtual reality" by the Syrian dictator Bashar al-Assad.[53] IHS Jane's intelligence briefing suggests that the modus operandi of the SEA is mainly carried out via "phishing emails, luring recipients into clicking links or entering login details for sites the SEA is trying to vandalize, which it captures."[54] Its cyber operations record has a sensational target set that includes The Washington Post, UNICEF, the U.S. Army website, Le Monde, International Business Times, and Reuters.[55] The group even has a volunteering section on its homepage along with a link for leaks.[56]

Open source intelligence suggests that the SEA is a cyber proxy war campaign by the Baathist Regime. According to The New York Times, "If researchers prove the Assad regime is closely tied to the group, foreign governments may choose to respond because the attacks have real-world consequences. The S.E.A. nearly crashed the stock market, for example, by planting false tales of White House explosions in a recent hijacking of The A.P.'s Twitter feed."[57]

It is known that the Syrian Computer Society (SCS), a tech group that was established by the late Bassel al-Assad and previously headed by Bashar al-Assad, provided the basis for SEA.[58] Furthermore, the Rami Makhlouf's connection warrants attention. The Makhlouf family, to which Bashar al-Assad's mother Anisah belongs, has always been a key player in the regime's inner circle. For example, Rami Makhlouf's brother, Hafez Makhlouf, was head of the internal branch of Syria's notorious General Security Directorate. Moreover, generals from the Makhlouf line, such as the former commander of the elite 105th Brigade of the Presidential Guard Brigadier General Talal Makhlouf hold an important position within the regime's military structure and are also accused of systematic crimes against humanity during the course of the civil war.[59] Coming from such a dark family legacy, Rami Makhlouf was seen as the key financial powerhouse of the Baathist regime and served as "an interlocutor between foreign investors and Syrian companies."[60]

At this point, the role and evolution of the SCS becomes crucial. Bashar al-Assad assumed the presidency of the Syrian Computer Society in the 1990s. The project was designed to serve two purposes, by Bashar's late brother Basel in 1989, who died in a car accident in 1994. On the one hand, it was a controlled and gradual charm offensive and social development program that aimed to introduce computers and internet into daily Syrian life, albeit in a manner that a Baathist dictatorship could manage.[61] On the other hand, in a non-kinetic fashion, it was intended to be an information warfare and psychological operations base to counter anti-Baathist propaganda in the internet.[62]

The SCS link to the Syrian Electronic Army shows that society adopted a cyber warfare mission under civil war conditions and began to run Baathist military campaigns in the fifth domain of fighting wars: cyber space. This study will argue that the Baathist Regime of Syria has developed a high level expertise in cyber operations during war-time situations and that their current cyber capabilities can be improved upon to a menacing extent if the regime remains intact. Furthermore, allies of the regime, especially China and Iran, enjoy formidable cyber warfare capabilities, which could translate into foreign assistance in the regime's hostile cyber activities.

Apart from the SEA and SCS, the ISIS-affiliated Cybercaliphate is another important actor to which Turkey must pay attention. The most sensational cyber operation of the group was the hacking of French television network TV5 Monde on April 8, 2015, with the hijacked message of "Je suis IS."[63] More threateningly, the Cybercaliphate uploaded the reported personal IDs and resumes of French soldiers who fought in anti-ISIS operations.[64] Even more concerning, the radical extremist hacker group hacked the official Twitter account of the U.S. Central Command in early 2015.[65]

Indeed, ISIS has proven a much higher and more threatening presence in cyber space that should be taken seriously. As underlined by Hoffman and Schweitzer in April 2015:

> "Although the use of cyber space by jihad organizations is not new, ISIS uses the internet, and primarily social media, more than any other terrorist organization before it. In addition to the organization's technological capabilities, it appears that its primary innovation in its use of cyber jihad is its role in transforming ISIS from yet another Islamic fundamentalist terrorist organization into a global brand name that features prominently in the public discourse in the West, as well as in the Muslim world. As part of its efforts to influence Middle East and global public opinion and brand itself, ISIS disseminates propaganda materials using a well-designed online magazine in English called Dabiq and produces high quality movies that are disseminated on YouTube, Twitter, and various websites affiliated with the organization. Furthermore, the organization targets and exploits online social networks for its own needs on an unprecedented scale. ISIS makes extensive use of Twitter, Facebook, Tumblr, and Instagram, and according to senior American officials, operatives and supporters of the organization produce up to 90,000 tweets every day. A recent extensive study found that ISIS supporters operate at least 46,000 independent Twitter accounts, with 200-500 of these accounts active all day, thereby helping to disseminate the organization's propaganda. …In addition to the extensive use of social media by the organization's operatives and supporters, ISIS' cyber jihad includes offensive use of online space for attacks on websites."[66]

The Cybercaliphate's activities could pose a great threat to Turkey by igniting more extremism among religious youth, especially because Internet use in Turkey is higher than its Middle Eastern neighbors. Turkey could also face cyber attacks, which may target official websites and mainstream media networks.

5.1. The 2008 Pipeline Attack and the 2015 Blackout: A Cyber Wake-up Call for Turkey?

In regards to direct cyber attacks and hostile activities targeting Turkey, this study will shed light on two incidents: the 2008 explosion at the Baku-Tblisi-Ceyhan oil pipeline and the 2015 blackouts through Turkey. The first incident is the 2008 explosions at the Baku-Tbilisi-Ceyhan (BTC) pipeline near the eastern Turkish city of Erzincan. Pipelines have always been vulnerable to terrorist attacks in Turkey. A security survey suggests that between the years 1987 and 2010, 59 sabotage plots were perpetrated on targeting the Turkish pipelines, and 19 of the total 59 sabotages took place between 2007 and 2010.[67]

The 2008 attack, however, was not business as usual. According to some news sources, "Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line, according to four people familiar with the incident who asked not to be identified because details of the investigation are confidential. The main weapon at valve station 30 on Aug. 5, 2008, was a keyboard that shifted the internal pressure of the pipeline systems, which led to the massive blast."[68] The attack on the oil pipeline coincided with Russia's Georgia campaign in 2008, drawing suspicion since the BTC pipeline was running counter to Moscow's energy geostrategic interests in Eurasia.[69] It was revealed that there was indeed intense efforts to jam the pipeline facility, cutting off alarm systems and all communications, including those linking data to the satellite systems.[70]

The hackers deleted all security camera records, except one recorded by an infrared camera that clearly shows two people with laptops walking near the facility.[71] Prior to the Russo-Georgian War in 2008, Ankara's ties with Tbilisi were fairly warm, and the Turkish administration was in support of Georgia's accession to NATO. In this respect, it is equally important that during the course of the war, some Russian sources openly accused Turkey, claiming that Ankara played an important role in improving and encouraging Georgia's military capabilities.[72]

The second sensational cyber attack claims surfaced following the recent blackouts that affected 44 of the 81 provinces in Turkey on March 31, 2015. This time, the suspicion of a cyber attack was openly voiced by Prime Minister Ahmet Davutoğlu, and some press sources claimed that Iran was behind the attacks as a response to President Erdogan's accusation of Tehran for its regional dominance assertions along with his remarks in support of the ongoing operations in Yemen.[73] The day-long blackout halted production in 298 organized industrial zones and cost some $700 million.[74] Some experts presented an even more pessimistic damage assessment, estimating around $1 billion in losses emanating from the blackout.[75] Moreover, the fact that the eastern city of Van, which directly receives electricity from the Iranian electricity grid, was not affected by the blackout causes even more suspicion.[76] Yet, there is no adequate evidence to openly accuse Tehran.

In a 2010 study, James Andrew Lewis, a cyber expert at the Center for Strategic and International Studies (CSIS), underlined why electrical grids can become targets for cyber attacks:

> "The electrical power system has always been a high priority target for military and insurgents. It is cheap and easy for insurgents to blow up or simply pull down pylons and transmission lines or to attack power plants and substations. This is a normal part of guerrilla warfare. Militaries also normally plan to attack power plants, substations or hydroelectric facilities as part of a bombing campaign. … The Aurora tests conducted at Idaho National Labs a few years ago showed it is possible to exploit remote access to send commands to large generators that cause them to damage or destroy themselves. Researchers were able to remotely change the operating cycle of the generator, sending it out of control. A video of the incident shows that the target generator shakes, emits smokes, and then stops. … There is evidence that unknown foreign entities have probed the computer networks of the power grid. Some electrical companies report thousands of probes every month, although we do not know whether these were cyber crime or part of a military reconnaissance effort. There is also anecdotal reporting that potential military opponents have done the reconnaissance necessary for a cyber attack on the power grid, mapping the underlying network infrastructure and locating potential vulnerabilities."[77]

Strategically, electricity grids are high-value targets that can trigger a series of direct and indirect damage to the adversary. From a military perspective, the two optimal options to inflict the most damage to the grid is either high-altitude nuclear detonation or cyber warfare. States like Russia, China, Iran, and North Korea have hinted at their intentions to attack grids within the critical national infrastructure target set.[78]

5.2. Turkey's Quest to Boost its Cyber Capabilities

The possibility that the March 2015 blackout was a cyber attack was not taken as seriously as the 2008 pipeline explosion. Even if the blackout did not result from a cyber attack, it should be recognized as a wake-up call and prove the feasibility of a cyber attack that could cost around $1 billion a day, paralyze life in Turkey's urban centers and inflict damage. Since then, a wave of cyber attacks targeting Turkey's official Internet networks and websites have been detected since May 2015. The hostile activity was orchestrated by twelve "cyber warfare jump-off points" simultaneously.

The reported Baku-Tblisi-Ceyhan oil pipeline cyber attack in 2008 offered invaluable lessons for Turkish decision-makers. First, it was important for showing the kinetic effects of hostile cyber activity. Second, the attack pointed out the link between regional security issues, energy geopolitics, and political/military competition. Third, the cyber attack exposed the vulnerability of critical national infrastructure to the emerging threats of the fifth domain of war.

In response to the BTC attack, Ankara decided to boost its cyber defense capabilities. In 2010, Turkey's National Security Council (MGK-Milli Güvenlik Kurulu) took its first steps towards building cyber capabilities, leading to the establishment of the Cyber Command of the Turkish Armed Forces in 2012.[79] In 2011, Turkey conducted its first National Cyber Security Drill that included both hypothetical scenarios and actual red-team hostile activities.[80] Four years later, cyber security was supposedly incorporated into Turkey's famous "Red Book," the classified National Security Policy Document (Milli Güvenlik Siyaset Belgesi) that provides doctrinal principles and strategic guidance to the Turkish state's agencies and institutions.[81]

6. Conclusion and Policy Recommendations

From a military standpoint, it would be fair to say that a high-profile cyber weapon is the combination of a nuclear weapon, a biological weapon, a time bomb, an anti-radiation missile, Special Forces, and a medieval sword. A high-profile cyber weapon resembles a nuclear weapon in its ability to devastate critical national infrastructure and is similar to a biological weapon in its intelligence requirements for detection of a strike and the identification of a perpetrator. Cyber weapons might be put in the same basket as anti-radiation missiles because of its ability to track signals and pave the ground for follow-up strikes. To a certain extent, they are reminiscent of time bombs for the gap between the time of attack and the moment of impact can be designed by the attacker. Because cyber weapons are clandestine operation assets, they are comparable to modern Special Forces. Finally, in terms of deterrence and the defense versus offense calculus, cyber weapons can be likened to a medieval knight's sword in that they cannot be deterred solely by handling a shield.

In light of these military evaluations, this paper concludes that cyber warfare is a complex phenomenon that transforms war beyond a mere technological shift. Cyber warfare does consist of a technological breakthrough in terms of kinetic and non-kinetic military capabilities that have brought about new doctrines, organizations, concepts, strategies and tactics, offensive and defensive approaches, and more importantly a new warrior-class; however, cyber warfare refers to a new domain for fighting wars. As noted earlier, domains of war are interrelated, and the trajectory of engagements is leaning towards joint warfare and combined operations concepts. In other words, concepts like Air-Land Battle, Air-Sea Battle, compel air, land, and naval units' operations to increasingly adopt a more joint character and further promote network-based operations. In the last century, space has been integrated into this complex picture and has become an invaluable part of operations in other domains.

As of today, advanced missions, such as missile defense or intercontinental ballistic missile (ICBM) launches, cannot be considered without employing space-based assets. Artillery systems, main battle tanks, and even modern infantry benefit from GPS-based systems, guidance, and tactical intelligence networks at theater level.

Due to drastic shifts in cyber interconnectedness and electronic high-tech infrastructure, cyber space is now following suit and being closely integrated into the other domains of war. In this regard, network-centric engagements are becoming more and more computerized in terms of Command-Control-Communications-Computers-Intelligence-Surveillance-Reconnaisance (C4ISR) infrastructure and precision-guidance munitions. Under these circumstances, cyber weapons are entering the picture with their ability to paralyze and blind enemy command and control nodes. Furthermore, electronic warfare (EW), an integral element of all military branches but especially for modern air forces, is building a closer relationship with cyber warfare. The same could be said for information operations and psychological warfare.

As a result, cyber warfare looms large both as a new domain and military technological breakthrough. Therefore, as the Revolution in Military Affairs theory necessitates, adaptation capacity is becoming not only a defensive must but also a way to gain significant and offensive upper hand for state and non-state actors. Turkey is no exception as it has begun to face complex cyber warfare threats in the 21st century. Turkish economic growth is highly dependent on energy infrastructure, electricity generation, and dams with high hydro-strategic value. Turkey continues to pursue strategic objectives, such as becoming an energy hub and commercial aviation hub for the country's powerhouse, Istanbul. Most of Turkey's state and private databases, banking and financial transactions, and information flow have been digitalized. Therefore, cyber security has become one of the main pillars of Turkey's security environment.

Accordingly, this paper suggests the following policy recommendations for Turkish decision-makers:

- This paper strongly endorses the establishment of a Cyber Command under the Turkish Armed Forces doctrinal order of battle. Deepened cooperation between Turkish Cyber Command, NATO's Cooperative Cyber Defense Center of Excellence, USCYBERCOM, and other allied cyber security organizations is encouraged.
- We appreciatively endorse the 2011 inter-agency cyber drill in Turkey. Unified efforts and cooperation in countering cyber threats are of critical importance. Unclassified information about Turkey's Cyber Command shows that there is no continuous and systematic red teaming and penetration testing. Thus, we suggest regular cyber drills with an effective red teaming activity.
- In light of emerging cyber security challenges, Ankara should renew its strategic calculus with regard to kinetic and non-kinetic threats to critical national infrastructure, sensitive information security, espionage and counterespionage activities, network-centric warfare, psychological warfare, information warfare, electronic warfare, and signal intelligence. For such a comprehensive transformation, we suggest establishing a multidisciplinary commission. The commission could answer to the Secretariat-General of the National Security Council (MGK) and be officially appointed to debate cyber issues at the highest level. Given that the MGK constitutionally assembles once every two months, the transformation agenda would allow a regular discussion and continuity on the subject.
- From a military theoretical and doctrinal perspective, this paper concludes that solely investing in cyber defense would be more or less trying to fly with one wing. Thus, this paper recommends finding a proper and legitimate legal framework for cyber offensive capabilities that would be in harmony with NATO capabilities.
- This paper strongly suggests establishing an inter-agency team comprised of military, law enforcement, internal security intelligence, foreign affairs, and legal bodies. Furthermore, the command level of Turkish Cyber Command could be graduated to higher levels in forthcoming years.
- Cyber security is an emerging area of expertise that is based on a multidisciplinary approach. Thus, we suggest setting new training programs for the Turkish security apparatus augmented by effective cooperation among academia, think tanks, and the private sector.
- The private sector and the state security apparatus are indispensable components of a holistic cyber defense and cyber security approach. Private organizations' cyber vulnerabilities can be exploited as cyber jump-off points by future adversaries. Additionally, security breaches can also serve subversive cyber espionage activities due to the interconnectedness of digital systems and rapid flow of information. Furthermore, Turkey does not have a clear organizational model or doctrinal approach for systematic cooperation between the private sector and state apparatus in terms of cyber security. Thus, this study strongly suggests the development of a comprehensive and holistic approach to handle cyber security and cyber defense issues both organizationally and culturally.
- Turkey's efforts for improving its cyber-defensive and cyber-offensive capabilities will be affected by NATO's perspective. NATO leaders are on the eve of making significant decisions on cyber issues in advance of the forthcoming 2016 Warsaw Summit. The said Summit can become a turning point for the development of NATO's cyber capabilities. The ongoing debate among NATO circles on this very issue has been centered on categorizing the cyber space as an equally recognized and operational field in addition to air, land,

and sea. Should cyber space become an equally recognized operational field for NATO operations, then the sharing of the Allies' cyber defensive and offensive capabilities can be undertaken akin to the current nuclear capabilities of the Alliance. Furthermore, NATO would be responsible with assisting Allied nations in terms of their cyber defense but also for setting out a roadmap, for the allied nations to improve their cyber capabilities.

- Turkey remains among the members of the alliance that champion a more assertive cyber doctrine for NATO. On the other hand, there are some NATO members, first and foremost the US that has opted for a more cautious approach, one that is undoubtedly based on a lack of enthusiasm for disclosing its own cyber capabilities and then being compelled to leverage them to help other NATO Allies. Other nations, such as France, have also resisted these attempts on different grounds that have more to do with favoring the European Union to lead cyber security efforts over NATO. However, prospects of an uptrend in cyber attacks remain highly likely in the foreseeable future, just like the recent incidents in Turkey in December 2015 Turkey. Thus, NATO leaders are expected to take firm decisions towards consolidating the Alliance's cyber doctrine, mission and capabilities at the 2016 Warsaw Summit. Such a decision would encourage Turkey to take further steps in the cyber field and to adopt a more consistent stance with regards to improving its cyber capabilities.

1- T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (Republic of Turkey Ministry of Transport, Maritime Affairs and Communication) "SOME-Sektörel Kurulum ve Yönetim Rehberi" (CERT-Sectoral Setup and Management Guide) 2014.

2- Turkey's National Action Plan on Cyber Security, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf, Accessed on: July 7, 2015.

3- http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Accessed on: June 29, 2015.

4- James A, Lewis., Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS, 2002. p.2.

5- Steven Metz and James Kievit., Strategy and Revolution in Military Affairs: From Theory to Policy, US Army SSI, 1995, pp. 2-3.

6- Andrew Krepinevich., "Cavalry to computer; the pattern of military revolutions." The National Interest n37 (Fall 1994 n37): 30(13). General Reference Center Gold. Thomson Gale. University of Florida. 19 Nov. 2006.

7- Barry D. Watts.,The Maturing Revolution in Military Affairs, CSBA, 2011, pp.15-20.

8- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, pp.28-29.

9- Paul J Springer., Thinking about Military History in an Age of Drones, Hackers, and IEDs, Air Command and Staff College, http://www.fpri.org/docs/springer1.pdf, Accessed on: July 7, 2015.

10- For a comprehensive assessment on the Roman light infantry, see: Adam, O. Anders., Roman Light Infantry and the Art of Combat, Cardiff University, 2011.

11- James A. Lewis., The Role of Offensive Cyber Operations in NATO's Collective Defense, The Tallinn Papers, CCDCOE, 2015, p.3.

12- John Arquilla and David Ronfeldt. "Cyber War is Coming" in In Athena's Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC 1997, p.24

13-Ibid. p.30.

14- Ibid.

15- Ibid. p.23.

16- Jennifer, J. Li and Lindsay Daugherty, Training Cyber Warriors, RAND, 2015, p.xi.

17- For detailed defense spendings see: IISS, Military Balance 2014.

18- US Cyber Command Fact Sheet, May 25 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces %20May%2021%20Fact%20Sheet.pdf, Accessed on: June 29, 2015.

19- Ibid.

20- http://www.al-monitor.com/pulse/originals/2015/06/israel-idf-cyber-intelligence-new-unit-eisenkot-war-future.html, Accessed on: June 29, 2015.

21- http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/24/israel-target-for-iranian-hezbollah- cyber-attacks/29210755/, Accessed on: June 29, 2015.

22- Joel Mullish. "Russia's Growing Reliance on Cyber Warfare Setting Dangerous Precedent for Future Foreign Policy", INSS, http://www.inss.org.il/uploadImages/systemFiles/Russia's%20growing%20reliance%20on%20cyber %20warfare%20setting%20dangerous%20precedent%20for%20future%20foreign%20policy.pdf, Accessed on: June 29, 2015.

23- NATO CCDCOE, https://ccdcoe.org/, Accessed on: June 29, 2015.

24- NATO, Cyber Security, http://www.nato.int/cps/en/natohq/topics_78170.htm, Accessed on: June 29, 2015.

25- Magnus Hjortdal., "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", Journal of Strategic Studies, Vol: 4 No: 2, Summer 2011.

26- For detailed information see: Mandiant, APT1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, Accessed on: July 28, 2015.

27- Eric, M. Hutchins et.al. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven- Defense.pdf, Accessed on: July 29, 2015.

28- Ibid.

29- Larry M. Wortzel., The Chinese People's Liberation Army and Information Warfare, US Army SSI, 2014, pp.1-8.

30- Ibid. pp.12-13.

31- Ilan Berman., The Iranian Cyber Threat Revisited, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cyber security, Infrastructure Protection, and Security Technologies, 2013, p.2.

32- James Andrew Lewis., Cyber security and Stability in the Gulf, CSIS, January 2014.

33- Executive Cyber Intelligence, INSS-CSFI, April 1st, 2015.

34- Jason, P. Patterson and Matthew, N. Smith., Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran, Naval Postgraduate School, 2005, p.44.

35- Ibid, pp.44-50.

36- James Andrew Lewis., Cyber security and Stability in the Gulf, CSIS, January 2014.

37- Craig Stallard., At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force, School of Advanced Air and Space Studies, Maxwell Air Force Base, 2011, pp.35-36.

38- Ibid.

39- Ibid.

40- Martin, C. Libicki., "The Specter of Non-Obvious Warfare", Strategic Studies Quarterly, Fall 2012.

41- Samuel Liles. et.al. "Applying Traditional Military Principles to Cyber Warfare", 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012, p.171.

42- Jeffrey R. Witsken., Network-Centric Warfare: Implications for Operational Design, School of Advanced Military Studies-US Army Command and General Staff College, 2002, p.3.

43- Ibid. pp.17-18.

44-Alvin L. Bailey., The Implications of Network Centric Warfare, US Army War College, 2004, pp.2-3.

45- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Vol: 3 No: 1, May 2011.

46- Erik Gartzke., "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", University of California, 2012, p.25.

47- Andrew F. Krepinevich., Cyber Warfare: A Nuclear Option, CSBA, 2012, p.66.

48- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, February/March 2012, Vol: 157 No: 1, p.6.

49- Austin Miller. Advanced Anti-Radiation Guided Missile: Strengthening DEAD Capability in the Fleet, 43rd Annual Systems: Gun and Missile Systems Conference and Exhibition, April 21-24 2008 Brief.

50- Thomas Rid and Peter McBurney, "Cyber Weapons", The Rusi Journal, February/March 2012, Vol: 157 No: 1, p.8.

51- Lior Tabansky., "Basics Concepts in Cyber Warfare", Military and Strategic Affairs, Vol: 3 No: 1, May 2011.

52- "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler" (The Importance of Cyber Security for National Security and Preventative Measures) Güvenlik Stratejileri (Security Strategies).

[53] Jane's Intelligence Review, Middle East Conflict Spills into Cyber space, 2015, pp.3-4.

[54] Ibid.

[55] http://sea.sy/index/en, Accessed on: June 28, 2015.

[56] Ibid.

[57] http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=1, Accessed on: June 28, 2015.

[58] Ibid.

[59] Human Rights Watch, By All Means Necessary: Individual and Command Responsibility for Crimes Against Humanity in Syria, 2011, p.87.

[60] Jeremy M Sharp., Unrest in Syria and U.S. Sanctions Against the Assad Regime, Congressional Research Service, 2011, p.4.

[61] It should be noted that by the mid 1990s, there was only two computers for 1,000 in Syria, and it was in 1997 that a pilot group of 400 Syrians were allowed to access internet.

[62] John B Alterman., New Media New Politics: From Satellite Television to the Internet in the Arab World, Washington Institute for Near East Policy, 1998, pp.40-41.

[63] http://rt.com/news/248073-islamic-state-hackers-french-tv/, Accessed on: June 28, 2015.

[64] Ibid.

[65] http://rt.com/usa/221927-central-command-hackedcybercaliphate/, Accessed on: June 28, 2015.

[66] Adam Hoffman and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)", Strategic Assessment, Vol: 18 No: 1, April 2015, p.73.

[67] USAK, "Kritik Enerji Altyapı Güvenliği Sonuç Raporu" (Critical Energy Infrastructure Security Final Report).

[68] http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, Accessed on: June 29, 2015.

[69] Ibid.

[70] http://www.milliyet.com.tr/siber-savasin-miladi/dunya/detay/1982549/default.htm, Accessed on: June 29, 2015.

[71] Ibid.

[72] http://www.hurriyet.com.tr/dunya/9623756.asp, Accessed on: June 29, 2015.

[73] http://www.dailysabah.com/diplomacy/2015/04/28/iran-allegedly-behind-nationwide-power-outage, Accessed on: June 29, 2015.

[74] http://www.hurriyet.com.tr/ekonomi/28611619.asp, Accessed on: June 29, 2015.

[75] "Elektrik Altyapısı ve Siber Güvenlik" (Electric Infrastructure and Cyber Security). http://www.edam.org.tr/tr/IcerikFiles?id=1028, Accessed on: August 3, 2015.

[76] http://www.hurriyet.com.tr/gundem/28604226.asp, Accessed on: June 29, 2015.

[77] James A. Lewis., The Electrical Grid as a Target for Cyber Attack, CSIS, 2010.

[78] Cynthia E. Ayers and Kenneth D. Chrosniak., Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency, US Army War College Center for Strategic Leadership and Development, Issue Paper, Volume 1-13, 2013.

[79] http://www.radikal.com.tr/teknoloji/tskda_siber_ordu_icin_onemli_adim-1194093, Accessed on: June 29, 2015.

[80] Information Technology and Communication Agency (Bilgi Teknolojileri ve İletişim Kurumu), http://www.tk.gov.tr/sayfa.php?ID=28, Accessed on: June 29, 2015.

[81] http://www.haberler.com/tsk-siber-savunma-komutanligi-ndan-hacker-atagi-7035427-haberi/, Accessed on: June 29, 2015.