Turkey—Challenges to the Struggle against Cyber Threats

Ofir Eitan

Turkey is one of the most technologically, economically, and institutionally developed countries in the Middle East. At the same time, it is one of the countries most exposed to cyber threats. The Turkish government has taken steps in recent years to narrow the existing gaps in defense against cyber threats, but its efforts in this area have not yet produced the desired results. This article analyzes Turkey's national cyber defense deployment and cites a number of structural challenges resulting from long-standing Turkish policy. The Turkish government will have to find solutions to these challenges in order to achieve the goals of its national cyber defense programs.

Keywords: Cyber, Turkey, policy, national security, political economy

Introduction

Cyber threats have had a growing influence on our lives in recent years and thereby on policies of many governments. Many countries accordingly have begun taking steps for devising a national strategy in cyberspace and forming infrastructure to defend against cyberattacks. Since reports of Stuxnet, Flame, and Shamoon in the media and of distributed denial-of-service (DDoS) attacks against the US financial sector, it has appeared that the Middle East has also become an active player in the lively cyberwar theater. The identity of the attackers in cyberspace is an ambiguous question, but the United States,

Ofir Eitan is a certified information and cyber security manager and a cyber threat intelligence officer with the rank of major in the IDF reserves. He has a BA and an MA in the history of the Middle East from Tel Aviv University.

Israel, Iran, and other countries in the Persian Gulf have nevertheless been mentioned in this context in recent years.

Turkey is one of the most developed countries in the Middle East, a regional power, and an important member of NATO; nevertheless, there is a major deficiency in the capabilities of its institutions to cope with cyberattacks. For example, only in 2016 was a national center established for coordination and cooperation in defense against cyberattacks. Only in July 2017 was the Turkish cabinet presented with a draft bill for strengthening defense of cyberspace in public agencies, by integrating security experts from various disciplines, including white hat hackers, professionals whose job is to improve the level of network computer security through controlled penetration tests and risk assessments. The aim of this measure was to expand the authority of the National Intelligence Coordination Center (NICC), a department subordinate to the Information and Communication Technologies Authority of Turkey (Bilgi Teknolojileri ve İletişim Kurumu [BTK]), which is responsible for handling and responding to cyberattacks throughout the country and for distributing actionable information and helping to protect all public agencies.[1]

Turkey has not yet consolidated a national protective framework in cyberspace incorporating the ruling institutions, security agencies, national infrastructure, and private entities, even though long ago it had formulated a national strategic plan in this matter, the 2016–2019 National Cyber Security Strategy and Action Plan.[2] The Turkish plan resembles similar processes that have developed in other countries in the western world, while considering the specific situation in Turkey, which must cope with diverse and constant cyber threats to the country's infrastructure.

Beyond the bureaucratic barriers, Turkey faces structural challenges that obstruct the steps necessary for the growth of high-level local infrastructure in the cyberspace. The internet and data communications sector, which is one of the industries that is knowledge-intensive, has unique characteristics that differ from those of other industrial sectors. As a result, the sphere of cyber warfare—the world of virtual attacks on computer systems and the

1 Şeyma Nazli Gürbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism," *Daily Sabah*, August 10, 2017, https://www.dailysabah.com/war-on-terror/2017/08/11/turkey-adopts-cybersecurity-strategy-fights-cyberterrorism.

2 Merve Seren, "Turkey Steps up Counter-Cyber Attack Efforts," *New Turkey*, January 24, 2017, https://thenewturkey.org/turkey-steps-up-counter-cyber-attack-efforts/.

defenses against those attacks—requires a special allocation of resources, particularly for the development of human capital.

Given these basic insights, I argue that Turkey's long-term centralized policy is responsible for the fundamental challenges that the country faces today in dealing with cyber threats to its national infrastructure. These challenges can be separated into two spheres that greatly affect Turkey's ability to develop its power in cyberspace: the policy and bureaucratic challenge and the organizational culture.

The analysis begins with a brief description of the state of Turkish national policy in the field of cybersecurity. The above-mentioned two spheres that contain the structural challenges facing Turkish decision makers in developing power in cyberspace are then analyzed. This essay relies upon a number of basic assumptions from the capitalist economic approach for the purpose of theoretically analyzing the development of the challenges facing Turkish policy.

Turkish National Cybersecurity Policy

Studies in recent years have presented data that should keep Turkey's defense leadership and its decisions makers awake at night. For example, as early as 2012, it was reported that Turkey was among the ten most attacked countries in the world in the cyberspace.[3] Some of the world's leading information security and communications companies, such as Trend Micro, Fortinet, and Akamai, reported in 2016–2017 that Turkey headed the list of countries in Europe and worldwide that had been most frequently cyberattacked.[4]

An analysis of the cyber threat landscape shows three main players threatening Turkey's governmental and commercial internet networks: political Kurdish players, the Gülen movement (FETO by the Turkish government), and cybercrime. An example of a Kurdish cyber threat was the widely-reported attack against the website of the Turkish Ministry of Finance, which had been defaced with propaganda corresponding to the agenda of the PKK, the underground Kurdish organization, and caused it to crash.[5] In this

3 Aydin Albayrak, "Turkey among Top 10 Countries Subjected to Cyber Attacks," *Sunday's Zaman*, July 1, 2012.

4 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

5 Umit Kurt, "Cyber Security: A Road Map for Turkey," Strategy Research Project (Carlisle, PA: US Army College, 2012), pp. 8–9; Ümit Enginsoy, "Turkey Centralizes Efforts for National Cyber Security," *Hurriyet Daily*, November 21, 2011.

event, the objective behind this "noisy" attack was clear, but the question of the attacker's identity in the cyber world usually remains unsolved. In this context, other famous attacks can be named, which were directed against Turkish government websites, such as those of the Ministry of Finance,[6] the national police and Turkish Airlines.[7] It is reasonable to attribute these attacks and others like them to Kurdish players as well as cyber criminals.

As using computer and communications networks by institutions and companies in Turkey increases, so does the threat to their proper functioning. It is believed that of the approximately 80 million residents of Turkey, the world's twentieth largest population,[8] nearly 43 million use the internet, putting Turkey in nineteenth place worldwide in the use of this communications medium.[9] This means that Turkey ranks alongside the most developed countries in the family of nations in relation to the number of residents and the extent of internet use. At the same time, however, Turkey lags behind in its national effort to defend its networks against cyberattacks, in comparison with the measures taken by other developed countries.

In October 2010, the Turkish army published the "Red Book," which provides a close-up once every few years of Turkey's national defense strategy. This book suggests that from Turkey's perspective, cyberspace is perceived as a non-conventional threat. In 2011, the Turkish National Security Council accordingly ratified a new national strategy that for the first time also included the problem of cyber threats.[10] As mentioned, a national plan for cyber defense strategy in 2016–2019 was also recently published.[11] This strategy has two main goals. The first is Turkey's recognition that cyber defense is an integral element of national security. The second is to bring Turkey up to par in the qualifications needed concerning the administrative

6 Kurt, "Cyber Security: A Road Map for Turkey."

7 Albayrak, "Turkey among Top 10 Countries Subjected to Cyber Attacks."

8 The figure is correct as of 2009, and it likely that the current number of users is even greater. In any case, this does not materially alter the picture.

9 Central Intelligence Agency, *The World Factbook*: *Turkey*, January 7, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html.

10 James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare*: *Preliminary Assessment of National Doctrine and Organization* (Washington DC: Center for Strategic and International Studies, 2011), p. 20.

11 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

and technology measures essential for achieving absolute security for all the national assets in the cyber realm.

The Turkish government institutions have de facto developed cybersecurity functions that are the result of an independent initiatives by government entities; indeed, there is no single authority or supreme agency in Turkey that coordinates national cybersecurity. Among the existing agencies are the Turkish national Computer/Cyber Emergency Response Team (TR-CERT),[12] which operates under the Information and Communications Authority, as well as the first Cyber Fusion Center, belonging to the Turkish Ministry of Defense.[13] Although activity in this sphere relies mostly on imported products, the Turkish army and the National Intelligence Organization (MIT) rely on local technological solutions for cyber defense developed and provided by Havelsan, the "government company for software and systems."

Following the staff work conducted in 2010–2011, Turkey devised a plan for establishing a "Cyber Command" in the Turkish army general staff for the purpose of repelling network attacks against the country. The general staff of the Republic of Turkey announced the establishment of this command in 2013.[14] Media reports and the statement of a senior Turkish army officer shed light on the situation behind the scenes of this new command. This agency, which is constructed along the lines of its American counterpart, has the job of monitoring the entire public internet in Turkey in order to provide a defensive framework for state institutions.[15] The Turkish "Cyber Command" is designed to act in cooperation with the Turkish Ministry of Defense, the National Council for Science and Technology Research (TÜBİTAK), and the Middle East Technological University. This command—headed by an officer with the rank of general—relies on a special budget, is independent in

12 CERT—Computer/Cyber Emergency Response Team is a concept first formulated by Carnegie Mellon University that refers to the need to establish national, institutional, or sectoral centers whose job is to assist targeted communities to prepare for cyber threats and how to cope with them.

13 Seren, "Turkey Steps Up Counter-Cyber Attack Efforts."

14 Burak Ege Bekdil, "Cyber Defense 'Indispensable Part' of Turkey's National Security: Senior Official," *Atlantic Council, Defense News*, December 13, 2013, http://www.atlanticcouncil.org/blogs/natosource/cyber-defense-indispensible-part-of-turkey-s-national-security-senior-official.

15 Kurt, "Cyber Security: A Road Map for Turkey," p. 14; Enginsoy, "Turkey Centralizes Efforts for National Cyber Security."

organizational structure, and includes a special cyber defense unit.[16] According to a statement by the Turkish minister of communications and transportation, Turkey's cyber defense program was put into practice in 2013.[17]

Awareness in Turkey of the need for defense of cyberspace and the potential of the threats in this sphere has increased in recent years, as can be seen from the policy plans and various local initiatives by governmental entities, but from a practical standpoint, Turkey's national cyber defense deployment lags significantly behind in comparison with other western countries. Çetin Kaya Koç, a professor of cryptography at the University of California, described well the situation in cyber defense: "Since Turkey did not complete its cyber transformation in its infrastructure yet . . . in case there is an attack on the infrastructure in the future, such as on metro systems or electricity, there are not enough precautionary measures taken to deal with it."[18]

This situation shows that progress in Turkey's cyber security mechanisms requires not only expediting the bureaucratic processes but also relying on two cornerstones of the country's national resources: trained local personnel and a local infrastructure of research and development. At the same time, as already noted at the beginning of this article, Turkey is obliged to meet many other challenges, resulting from the centralized policies of its government since the establishment of the republic; these challenges create barriers and obstacles that delay the consolidation of these two cornerstones.

The Challenges Facing Turkey in Developing Cyber Power

The capitalist approach to political economy holds that a centralized policy constitutes one of the market failures, delaying manufacturing and technological development and the growth of private entrepreneurship. The philosopher and economist Adam Smith argued that a division of labor between all market players leads to professionalism, saves time in the transition between the various stages of production, and motivates people to perfect production processes. In addition, the capitalist approach does not dispute that the state has an important role to play in economic development and stabilization,

16 Lewis and Timlin, *Cybersecurity and Cyberwarfare.*

17 "Turkey's Cyber Defense Plan to be Ready in 2013," *Hurriyet Daily*, March 2, 2012.

18 Gürbuz, "Turkey Adopts Cybersecurity Strategy, Fights Cyberterrorism," *Daily Sabah*, August 10, 2017.

even in the free market era of our time. In this framework, the state exerts an influence through regulation of the labor market, education, professional training, and so forth, while setting economic policy, passing legislation, and creating enforcement measures within the framework of the tension between the market's decentralization and its centralization.[19]

In a liberal market economy, firms solve market failure through reciprocal relations within the free market, contracts (arrangements), and hierarchy (relations between firms). In other words, according to the classic liberal approach, market failures are solved by the dynamic of the "invisible hand" of market forces. In the coordinated market economy typical of Turkey, firms rely less on competition and more on business networks and reciprocal strategic relations ("incomplete contracts"). In practice, even under the dictates of the free market, centralization in the economy is preserved in the hands of the state and a few powerful economic groups.[20]

The Policy and Bureaucratic Challenge

Until the late 1990s, the Turkish government did not adopt any deliberate policy to encourage private entrepreneurship in general, and high-tech industries in particular. This was the result of a policy of many years standing, originating from the time of the transition from the Ottoman Empire to the modern Turkish Republic. Even thought the Turkish Republic inherited a tradition more than a century old of adopting western technology, its foundations were built upon an impoverished country whose economy rested on agriculture and the absence of any institutionalized private-sector infrastructure.[21]

The first Turkish government following the dissolution of the Ottoman Empire aimed for economic and social development but believed that it should consist of heavy industry focused on manufacturing. For this purpose, and as part of its general centralizing policy, the Turkish government founded government-owned and managed companies, while adopting five-year plans based on the Soviet model. In addition to its centralizing policy, which blocked

19 Peter A. Hall and David Soskice, "Varieties of Capitalism," *The Political Economy Reader*: *Markets as Institutions*, ed. Naazneen H. Barma and Steven K. Vogel (Indiana: Routledge, 2007), pp. 292–303, 307–312.

20 Ibid.

21 Arnold Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms? Or, Why is Turkey so Dependent on Technologic Innovations Created Outside its Borders?," *SSRN*, May 26, 2006, pp. 1–4, https://ssrn.com/abstract=904780.

any possibility of private entrepreneurship, all Turkish governments have adopted a development policy that does not accommodate demand for local development. As a result, the construction of Turkey's infrastructure has been based completely on imports. The Turkish government signed agreements with foreign corporations for designing, constructing, and operating large-scale ventures, which passed into Turkish hands at the end of the process. This process has persisted until today. This policy culminated in exclusive dependence on external technology and the absence of any need for local entrepreneurship.[22]

The Turkish government also replicated the format of establishing government companies and corporations in the private sector, with the state targets and the way in which they are implemented remaining identical. Up until the late 1990s, government support for the private sector focused on heavy industry with the main purpose being the creation of as many jobs as possible. This policy had additional consequences, two of which are important in this context. The first was the neglect of knowledge-intensive industries, for which trained, educated, and expert personnel is usually needed, in addition to fewer jobs in this sector than in other sectors. The second was the rise of a class of oligarchs. These were the heads and owners of the large corporations—a conglomerate of families—who shaped demands in the Turkish market according to their needs, and whose interests almost completely overlapped with those of the state. These corporations do not usually need engineers and high-tech personnel, and they therefore perpetuate the technological stagnation, the backwardness within the population, and the focus on blue-collar industries.[23]

Even after the opening of the Turkish market in the late 1990s, local entrepreneurs were confronted with a bureaucratic labyrinth that complicated and even thwarted any sign of local entrepreneurship. This is a significant challenge for the high-tech industries in general, especially the cyber and internet sector. From the beginning, a Turkish entrepreneur seeking to establish a startup finds it almost impossible to raise money other than personal or family capital. Most potential credit for initiatives of this type is in the hands of the banks, which pursue a cautious policy because of the frequent crises

22 Ibid.

23 Ibid, pp. 1–4, 9.

in the Turkish capital market over the past thirty years.[24] Statistics show that less than 5 percent of the available bank credit in Turkey is provided to industrial SMEs (Small-Medium size Enterprises). This is rather ironic, given the fact that SMEs account for 99.5 percent of the establishments in the industrial sector, 66.5 percent of employment in the sector, and 34 percent of value added in the sector.[25]

Even when the banks in Turkey decide to provide credit to business entrepreneurship, many of them are incapable of formulating a proper financing plan and of finding the relevant financial resources to pay for it. Furthermore, alternative sources of financing, such as venture capital funds, angel investments, and capital raising through share offerings are underdeveloped in Turkey in comparison to other western countries. In addition, most loans to entrepreneurial firms in the Turkish market are provided by Halk Bank, the Turkish national bank, which is in the process of privatization.[26] This contrasts with the sources of financing for entrepreneurs in western countries, which come from a broad range of financing and aid instruments, including the government itself, foreign investments, growth-encouragement companies, non-governmental organizations, international trade organizations, and so forth.[27] As noted, economic growth levers of this type are underdeveloped in Turkey. This situation poses many challenges and barriers to the high-tech industries in the country, including the cyber industry.[28]

In terms of the bureaucratic processes that a Turkish entrepreneur faces, it is worthwhile quoting the description of this substantial challenge by Dilek Çetindamar, a professor of management at Sabancı University in Istanbul, who said, "Turkey is the 13th most bureaucratic country in the world . . . an entrepreneur needs 172 signatures from various government agencies in order to receive approval to invest . . . in Turkey an entrepreneur spends 20% of his or her time on bureaucratic issues, this rate is 8% in the European Union."[29]

---

24 Ibid, pp. 8–9.

25 "Small and Medium-Sized Enterprises in Turkey: Issues and Policies," *OECD Report* (Paris: OECD Publications, 2004), pp. 2–33.

26 Ibid.

27 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

28 "Small and Medium-Sized Enterprises in Turkey."

29 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

Another critical aspect in the free market era is the lack of access to information among Turkish startups. According to neo-liberal economic principles, promotion of economic growth requires the opening of most information and knowledge channels. A study by the OECD (Organization for Economic Development and Cooperation) in 2004 of the small and medium-sized enterprises sector found that the Turkish market lacked knowledge-based agents and communications channels for information sharing. The OECD recommended that the Turkish government refrain from conflicts between legislative bodies and law enforcement agencies over conflict of interest in order to facilitate transparency for the benefit of small and medium-sized enterprises.

In 2001, with the start of the national program for implementing the Treaty on European Union (the Maastricht Treaty), Turkey pledged to undertake basic reforms of its local regulation systems according to the accepted international criteria. This process, together with other measures that the Turkish government is trying to advance, is designed to improve bureaucratic processes and the regulatory systems in Turkey, among other things.[30]

The Organizational Culture Challenge

The cyber realm is notable for its human capital, which distinguishes the know-how and specialists in this sector from the other high-tech industries. Among other things, several characteristics or professional traits are necessary for the development, progress, and attainment of an appropriate level of software engineers, communications network specialists, information security experts, as well as hackers. These are not scientific measures but rather an institutional and organizational environment that generates and facilitates the growth of innovative developments and technological solutions. It is difficult to separate this essential element of the cyber sector from the centralizing institutionalized policy typical of Turkey, because according to the liberal approaches to political economy, a centralizing policy creates barriers to the development of firms and individuals in the internet and data communications sectors that are seeking to break through and innovate in their field.

In order to assess the challenges of the organizational culture facing the creation of human capital in Turkey's cyber sector, the focus should be on two fundamental characteristics to this country: the relations between the

30 "Small and Medium-Sized Enterprises in Turkey"

state and the military and its research and development culture. Our basic assumption is that centralization in the Turkish establishment prevents structural processes (market failure) necessary for the growth of the cyber industry in the country.[31]

Many people regard the defense industries as a spur and catalyst for technological developments in many industrial sectors, especially in the knowledge-intensive industries. Taking this basic assumption into account, it would be logical to conclude that Turkey, in which the army constitutes a pillar of the regime and society, should also be a pioneer in the cybersphere, or at least have a high-quality "toolbox." The reality in the Turkish cybersphere, however, is very different. Prof. Arnold Reisman claims that Turkey has not succeeded in channeling its military effort and defense industries into the development of important technologies in the civilian market, which is essential for growth in the cyber industry. In order to prove his claim, Reisman conducted a theoretical comparison between three countries bearing similarities that are tangential to our discussion: Turkey, Israel, and Iran. Since gaining their independence, these three countries have continuously faced significant national security threats to their sovereignty, and all three have experience in absorbing and integrating high-quality weapons featuring sophisticated technology.[32]

Turkey's defense industries currently export independently developed products requiring highly technical professionalism in air and sea warfare, electronic warfare, and command and control systems.[33] However, the reciprocal relations between the Turkish defense industries and the private firms in Turkey (individuals and organizations) in cyberspace have not led to the development of an adequate "toolbox," because the government cyber industries, like every other technological industry in Turkey, are not developed sufficiently for this purpose. Reisman's findings show that Israel has successfully channeled its military developments for the purposes of both helping economic firms in the country and distributing technologies and know-how in the civilian market. In Turkey, on the other hand, such a process is almost totally absent. Like developing countries, Turkey has

31 Hall and Soskice, "Varieties of Capitalism."

32 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 10–15.

33 Ibrahim Sunnetci, "High-Tech in Turkey – Special Report," *Military Technology* 35, no. 3 (2011):107–110.

learned how to manufacture light weapons and ammunition, but it regularly purchases the more sophisticated weapons in its arsenal from other countries (including Israel).[34]

Prof. Reisman presents a theory for understanding this situation. He compares Israel's military and social fabric with that of Turkey, while emphasizing Israel's uniqueness as the "Startup Nation," although Turkey, like Israel, has compulsory military service. Most of the Israeli military's internal organizational research and development processes are based on the people serving in the army, but the uniqueness of Israel is that the dictates of organizational demand cause the military command to allow space for creativity and extensive action, and the organizational culture encourages the growth of bottom-up ideas and initiatives from within the ranks. When this organizational culture is combined with the fact that the Israeli army finds and selects the candidates from the majority of the population that has reached the age of eighteen and that a high proportion of young people serve in the army, fruitful reciprocal relations emerge between the army and civil society.

Indeed, many civilians in Israel after their military service move into the civilian market with a great deal of high-quality know-how and work experience. In this situation, many doors are open to them in order to channel their creativity for the benefit of civilian companies, some of which are headed by veterans of the security system. In Turkey, on the other hand, there is no such tradition nor is there a similar process of reciprocal fertilization between the military and the civilian market. Thus, even when the Turkish defense establishment spots people in the system with good qualifications, they ordinarily use those people if they choose to remain within the framework of the state-owned defense industries, which mostly operate under organizational and bureaucratic constraints and dictates that delay growth.[35]

Despite the above, it can be argued with a great deal of justification that the existence of close army-society relations does not necessarily create an echelon of excellent human capital for the cyber sector. Even though this axis generates development, various countries in the past and the present have reached a pinnacle of achievement even without the need to find a solution

34 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 10–15.

35 Hall and Soskice, "Varieties of Capitalism"; Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 5–8.

to security threats. The investments of both the Turkish establishment and the country's private firms in academic or commercial research are extremely meager. To this should be added the fact that the salaries of academic researchers in Turkey are not high, which tends to keep academic quality at a low level. The institutional organizational culture is not fertile ground for development, sharing of ideas, creation of information and knowledge, and so forth, which are all cornerstones for the progress and growth of the cyber industry.[36]

As a rule, neither the Turkish establishment nor Turkish tycoons have done enough over the years to foster research, development, and technological entrepreneurship. It is important to stress that the Turkish oligarchs do direct capital to the public and the market, but most of the contributions and investment funds are channeled into building schools, universities, and museums. Turkey has no institutionalized mechanism for empowering academic researchers through the private market or encouraging technological entrepreneurship wherever it might be. In order to highlight this, the first technological park in Turkey was founded in 1985 by the Technological University in Istanbul and the municipal chamber of commerce. A similar institution was founded in Ankara only in 1991 by the Middle East Technical University. In contrast, Prof. Reisman points out that the Weizmann Institute of Science, an institution established in Israel in order to export academic findings to the commercial market, among other things, began operating as early as the 1950s.[37]

I have seen fit to conclude this discussion with a quote from Prof. Reisman's research: "Although Turkey changed its government in 1923 and undertook major reforms, it did not change its people, who are steeped in tradition. Historically during the Ottoman Empire, educated Turks have been administrators, bureaucrats, and not business-minded[38] nor particularly technically inclined."[39]

---

36 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 5–8, 10–12.

37 Ibid, pp. 12, 15.

38 When Reisman uses the term "business-minded," I assume that he is referring to business thinking and entrepreneurship in the free market.

39 Reisman, "Why Has Turkey Spawned so Few High-Tech Startup Firms?," pp. 8–9.

Conclusion

Perusal of various Turkish sources in English shows that the academic discussion of the cyber question in Turkey still has not yet reached maturity. Even though quite a few news and media reports of cyberattacks experienced by Turkey can be found on the internet, it is clear that its discussion usually consists of opinion pieces written by various parties. In considering the main processes that Turkey has experienced in the cyber realm, I chose to focus on the challenges facing it, especially the lack of local human capital, which I believe is the core problem. I relied on an analysis of the situation, especially using the findings and conclusions of Prof. Arnold Reisman, together with the use the findings of the 2004 OECD report, which focused on research on the Turkish economy and on making of recommended course of actions for its development. Even though the academic discussion and the analysis I have set forth in these pages are incomplete, they indicate the need to gain a deeper understanding of the fundamentals of Turkish culture in order to decipher the basis for the challenges facing the development of the local cyber industry.

The distinction I proposed between the effect of the centralized Turkish policy on the political-bureaucratic challenge on the one hand and the organizational culture challenge on the other is a purely artificial distinction for the purpose of clarifying the logical argument. In practice, what is involved is a symbiotic relationship between the culture of Turkish society and its government's policy. The current socioeconomic situation in the country shows that a large percentage of the Turkish populations lives in a rural environment and maintains a traditional patriarchal Islamic society. This affects the policy and functioning of the Turkish governments.

The statement by Prof. Dilek Çetindamar describes the situation well: ". . . but rather that 'university graduates' career plans involve working in large companies, since starting up a firm is considered a big risk. Therefore, no tradition of entrepreneurship exists."[40] This statement expresses the main conclusion of this article: In order to foster high-level human capital in the Turkish cyber community, a suitable environment is needed; that is, an infrastructure that encourages initiative and innovation. It appears, however, that Turkey is not an "incubator" that encourages private entrepreneurship, which, according to the accepted formula, is a necessary condition for

40 Ibid, p. 14.

fostering pioneering high-tech personnel and engineers. Furthermore, when Turkey needs special technological solutions, it is likely to choose to import outside knowledge, and each one of the players in the triangle of the state, oligarchs, and society will prefer to channel human capital into the large manufacturing companies, while space for originality and entrepreneurship essential to the cyber realm will remain limited.