Broad Economic Warfare in the Cyber Era

Shmuel Even

Broad economic warfare encompasses a host of actions aimed at damaging or threatening to damage the economy of an enemy or rival, with the aim of pressuring or weakening it in order to achieve strategic aims. Broad economic warfare encompasses standard economic warfare (such as sanctions), kinetic warfare, and cyber warfare against an enemy's economy. The cyber era has changed the realm of broad economic warfare. From an offensive perspective, cyber capabilities make it possible to damage the enemy economy both during wartime and between wars. Cyber warfare can intensify the damage caused to an enemy's economy by economic sanctions and/or kinetic attacks. From a defensive perspective, cyber warfare poses another danger to the functioning of the economy. Although extreme scenarios of cyberattacks against the economies of countries have not occurred yet, it is necessary that the pace of building defenses for the state cyber system adapt to the rapidly accelerating establishment of the economy within the cybersphere.

Keywords: Broad economic warfare, economics, warfare, cyber, Israel, Iran

Dr. Shmuel Even is a senior research fellow at the Institute for National Security Studies.

Introduction

The purpose of this article is to present the concept of broad economic warfare and explore its application in the cybersphere. The article is divided into two parts. The first part defines broad economic warfare as encompassing all acts of warfare that target the enemy's economy. This field encompasses standard economic warfare (such as sanctions), kinetic warfare, and cyber warfare against an enemy economy. It is also characterized by defensive aspects. The second part of the article focuses on cyber warfare as one means of broad economic warfare and distinguishes between soft and hard warfare. The article discusses examples of different ways of implementing this kind of warfare.

Background

Strategies of warfare that are economic in character have been around since ancient times. In those days, the blockade was a common implement of warfare and the spoils of war constituted the supplies that advancing armies required and the remuneration enjoyed by the victors. Strategies of economic warfare have evolved since then, resulting from changes in the world's economic, political, and military realities. *Encyclopedia Britannica* defines economic warfare as "the use of, or the threat to use, economic means against a country in order to weaken its economy and thereby reduce its political and military power."[1] According to the *Oxford Dictionary*, economic warfare is "an economic strategy based on the use of measures (e.g., blockade) of which the primary effect is to weaken the economy of another state."[2]

It has been typical, at least in recent decades, to view standard economic warfare as limited to measures that do not use military force against the economy of the enemy; that is, attacking the economy of an enemy state using kinetic weapons in order to impair the production capacity of the enemy is not part of the toolbox of standard economic warfare. However, the use of the blockade, which is a military implement that could lead to the use of kinetic weapons within the framework of standard economic warfare, is somewhat ambiguous. This issue has also raised questions about

1 George Shambaugh, "Economic Warfare," *Encyclopedia Britannica*, https://www.britannica.com/topic/economic-warfare.

2 "Economic war," *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/economic_war.

the classification of high-intensity cyberattacks against economic targets of the enemy, of which the expected results are no less powerful than kinetic attacks. This includes, for example, cyberattacks against power stations, industrial plants, and transportation systems, damage to which is liable to have a kinetic effect (including the destruction of property and loss of life). In an analogy to kinetic attacks, therefore, cyberattacks of this kind are not found in the standard definition of economic warfare.

Given the above, we use the term "broad economic warfare" as a framework to encompass all the different kinds of measures designed to damage—or threaten to damage—the economy of an enemy or rival so that the party exercising the warfare can achieve its strategic aims. The distinction between broad economic warfare and standard economic warfare is summarized in the following table. As noted, broad economic warfare also has a defensive aspect.

Table 1. Broad Economic Warfare vs. Standard Economic Warfare

Category		Characteristic Measures
Economic Warfare (standard definition)		Various kinds of economic sanctions, such as the freezing of assets abroad, proscriptions in commerce and investments, discriminatory trade terms (not based solely on purely economic considerations), boycotts in various economic areas, embargos, and blockades aimed at preventing the enemy from engaging in trade.[3]
Broad economic warfare	**Soft Warfare**	Various kinds of economic sanctions, including freezing assets abroad, boycott, prohibition of trade, and embargo (not including kinetic damage to means of transport of the enemy). A downgrading of the conditions of economic relations with a rival for reasons that are not solely economic in nature, for example, in the realm of trade and investments. Information warfare and "soft" cyber warfare. Use of illegitimate means to achieve a strategic advantage, such as the large-scale theft of intellectual property.
	Hard Warfare	Closure/blockade using military forces aimed at preventing trade by the enemy, which may result in a military confrontation. Kinetic attacks on targets within the enemy economy. High-intensity cyberattacks against infrastructure and factories.

3 *Encyclopedia Britannica.*

Broad Economic Warfare: Definition, Attributes, and Goals

As already noted, broad economic warfare can be defined as measures aimed at harming, or threatening to harm, the economy of an enemy or rival,[4] to exert pressure on it or weaken so that the party exercising the warfare can achieve its strategic aims. This array also includes measures for defending against offensive actions taken by the enemy. In other words, broad economic warfare is a combined field encompassing all the measures of warfare that target the economy of the enemy. It includes sanctions, information warfare, boycott, embargo, military closure, kinetic warfare, and cyber warfare against the enemy's economy. It also includes defensive actions against such measures, such as the capability to respond, measures in preparation for sanctions, passive and active defense, and cyber defense of the economy.

According to the above definition, broad economic warfare is not limited to the standard tools of economic warfare but rather augments them with powerful kinetic and cyberattacks against targets within the enemy's economy. For example, measures against the enemy's electricity system may include ceasing the sale of electricity as a political sanction; sanctions on the import of spare parts for power stations; a cyberattack or kinetic attack that results in a temporary electrical outage; or a high-intensity cyber or kinetic attack that does irreversible damage to the turbine of a power station.

Broad economic warfare may be combined, in part or in full, with other types of measures depending on the goals, means, and strategy adopted. It may be part of "soft" warfare, such as combined with economic sanctions and cyberattacks on an economy with the goal of exerting heavy strategic pressure on the enemy without using military force. It may also be part of "hard" warfare and be carried out alongside high-intensity kinetic attacks and cyberattacks against the enemy's economic targets.

The goals of broad economic warfare are as follows:

1. To exert strategic economic pressure on an enemy or rival in order to change its behavior as desired by the party that is exercising the warfare.
2. To make it difficult to supply resources for the enemy's military buildup with the aim of weakening its force ("force design") and to damage the

4 For example, US president Donald Trump defined Russian president Vladimir Putin not as an enemy but as a rival, after the United States imposed sanctions on Russia. See "Trump Claims Victory in NATO: England will do something," *Ynet*, July 12, 2018, https://www.ynet.co.il/articles/0,7340,L-5308872,00.html [Hebrew].

enemy's economic resources, infrastructure, and assets in order to impair its military activity ("force use").

3. To undermine the status and stability of the enemy regime, to exert pressure on it to bring about a change in its priorities and policy (for example, in the case of the Iranian nuclear program), to strengthen the opposition against it, and even to bring about its overthrow.
4. To deter war or shorten its duration, to exact a price of war from the enemy, and to extend the time it takes it to rebuild itself in the aftermath—with the aim of delaying the outbreak of the next war.
5. To use the enemy's resources against it, or as compensation from it (for example, seizing funds in order to compensate the victims of terrorism).

The Means and Tools of Broad Economic Warfare

Broad economic warfare is divided into two categories: "soft" warfare, which does not make any direct use of kinetic force or the destructive force of cyber; and "hard" warfare, which involves different kinds of force, the intensity of which deviates from soft warfare.

Means of "Soft" Warfare

Soft warfare refers to economic warfare conducted by a single country or a group of countries, as well as organizations, with the aim of exerting significant economic and political pressure on a rival or enemy in order to weaken it and cause it to change its policy, without using military force.

Punitive Measures

These measures include sanctions, embargos, and/or boycotts of the economy of an enemy or rival, such as reducing or suspending economic relations (trade, banking, tourism, investments, and different types of economic agreements); imposing discriminatory import taxes for political reasons; pressuring companies and other countries to halt their economic relations with the enemy or rival country; distancing a recalcitrant country from the mechanisms of the international economy; and freezing the country's funds and assets held abroad. Examples of these measures include comprehensive sanctions imposed against Iran (including the ban on the export of Iranian

oil)[5] and against North Korea[6] due to their nuclear programs; US sanctions imposed on Russia due to its intervention in the US elections using cyber methods;[7] the freezing of Iraq's assets abroad following its invasion of Kuwait in 1990; the oil embargo imposed by the Arab states in 1974, which was intended to pressure the Western economy by creating an oil shortage and an increase in prices; and the boycott of Israel by the Boycott, Divestment, and Sanctions (BDS) movement.

Beyond the direct impact of punitive measures on the economy, such measures also are able to create an atmosphere of economic strangulation and a sense of no way out for the injured party. Still, researchers are divided as to the effect of sanctions, making it preferable to assess each case separately.[8]

Additional Soft Actions for Impairing a Rival's Economy

Other soft actions include cyberattacks aimed at disrupting sites that are essential to the state administration and the economy of the enemy or rival; information warfare aimed at undermining the strength of its economy (for example, by spreading distressing information regarding the low value of the currency, the weakness of the banking system, the flight of capital, and the shortage of food); interference in the enemy or rival's monetary system (for example, the Nazis' production of counterfeit British pound sterling notes during World War II); and acts of technological and industrial espionage between countries aimed at the large-scale theft of intellectual property in order to change the strategic economic balance between them, even though

5 Today, the sanctions are being imposed by the United States, which withdrew from the nuclear agreement with Iran. See, for example, Tal Schneider, "Everything You Need to Know about the Economic Sanctions to be Imposed on Iran," *Globes*, May 8, 2018, https://www.globes.co.il/news/article.aspx?did=1001235164 [Hebrew].

6 "The UN Unanimously Approves New Sanctions against Pyongyang," *Haaretz*, September 12, 2017, https://www.haaretz.co.il/news/world/america/1.4437072 [Hebrew].

7 Ran Dagoni, "As a Result of the Election Interference: The United States Imposes Sanctions on Russia," *Globes*, March 15, 2018, https://www.globes.co.il/news/article.aspx?did=1001228035 [Hebrew]; Missy Ryan, Ellen Nakashima, and Karen DeYoung, "Obama Administration Announces Measures to Punish Russia for 2016 Election Interference," *Washington Post*, December 29, 2016.

8 For theoretical background on the issue of sanctions, see Nizan Feldman, *In the Shadow of Delegitimization: Israel's Sensitivity to Economic Sanctions*, Memorandum no. 163 (Tel Aviv: Institute for National Security Studies, 2017), chapter 1.

information gathering is not considered an act of war. Broad economic warfare also includes the use of economic powers to weaken the enemy for political and/or military reasons, including the imposition of discriminatory import taxes.

Additional Matters

Many measures are conducted in the global economic realm, both in and outside the framework of agreements between countries, and while one party sometimes benefits and another loses, they should not be considered economic warfare. This stems from the observation that broad economic warfare aims primarily at achieving political and military goals, even if the party exercising the warfare faces economic costs.

From the perspective of the side plotting the war, broad economic warfare is not optimal. In contrast, in economic struggles—including trade wars—one side expects to achieve an economic advantage over its trading partners, some of which are allies, using customary measures of the world economy. One example of this approach is the protective tariffs that the US administration imposed on the companies of the European Union, Canada, and Mexico.

To complete the picture, it is also important to note the positive economic levers of influence. This is the flip side of broad economic warfare, although the goals of these levers are the same as those of the negative levers: to cause states and organizations to conduct themselves in the manner desired by the party using them. These involve the use of economic incentives to further military and political aims and they include aid in the form of grants and loans with comfortable terms, economic agreements, preferential terms of trade, the forgiving and spreading of debts, the conveyance of technologies, and more. Both parties may end up benefiting from the use of economic levers of influence: The party that exercised it enjoys political gain, whereas the other party enjoys economic gain. For example, the different forms of US foreign aid strengthen the Unites States' legitimacy to make demands of the countries receiving its aid.

By definition, economic levers of influence are not weapons. Still, some regard the cessation of economic incentives, the threat of such cessation, or the act of making aid conditional upon achieving political aims either as acts of broad economic warfare or as acts bordering on such warfare. For example, the American administration cut its aid to the Palestinians due

to their failure to cooperate politically with it, and Saudi Arabia links its economic aid to Jordan to its demand that Jordan promote Saudi Arabia's political and security aims, which is topped by the goal of curbing Iranian influence in the Middle East.[9] In addition, during the First Gulf War in 1991, the allies that fought against Iraq provided Egypt with billions of dollars of cash aid and slashed its debts to $25 billion, in exchange for its participation in the war against Saddam Hussein. Syria also received economic aid for taking part in the war.

Means of "Hard" Warfare

Military Blockade

A military blockade refers to the use of military force to prevent or limit the flow of goods and services between the enemy state and the rest of the world with the goal of exerting economic pressure on it, primarily to achieve political and military goals. This measure may sometimes also involve the use of kinetic weaponry.

A distinction can be made between a blockade against a recalcitrant state based on international agreements and rules—such as the international coalition's blockade of Iraq after its invasion of Kuwait in 1990—and the blockade that different states attempt to impose against the shipping routes of other countries as part of a war between them. Examples of the latter include the blockade that Iran imposed against Iraq's oil export routes by attacking oil tankers in the Persian Gulf during the Iraq-Iran War in the 1980s; Egypt's blockade of Israel's shipping routes in the Straits of Tiran in May 1967 (which was one of the main causes of the Six Day War); and Germany's use of submarine warfare to sink the commercial ships of its enemies during World War I and II.

Attacks on Infrastructural and Economic Targets

Attacks or the threat of such attacks on infrastructural and economic targets using kinetic weapons and/or high-power cyberattacks are carried out to weaken and deter the enemy, shorten the duration of the war, deter escalation, and raise the cost of the war. Examples include Israel's deterrence of Hezbollah by means of threatening to attack Lebanon's infrastructure; the US attack

9 Dan Arkin, "Economic Aid on Saudi Terms," *IsraelDefense*, June 13, 2018, http://www.israeldefense.co.il/he/node/34572 [Hebrew].

against Iraqi oil facilities during the First Gulf War; the Israeli Air Force's attack on strategic targets within Egypt and Syria during the Yom Kippur War (oil facilities, government institutions, refineries, and relay stations).

Economic Terrorism

Economic terrorism is the attack or threat of attack by terrorist organizations against a state's economic targets or against its sense of economic security. Examples include Hezbollah's threat to strike at power stations in Israel;[10] the "kite terrorism" launched from the Gaza Strip in the summer of 2018, which burned agricultural crops in the Negev; the theft and destruction of agricultural equipment in Israel for nationalist reasons; and terrorist attacks aimed at impairing tourism in Israel.[11]

Broad economic warfare can also be used against terrorist groups, as in the threat against the economy of a population who supports the organization in question (in the case of semi-state organizations), or damage to their sources of funding and financial systems (as implemented in the case of ISIS).

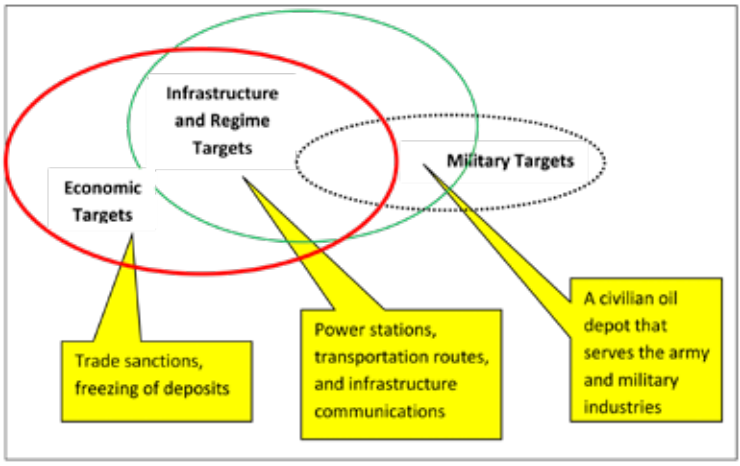

Figure 1. Targets of Attack of Broad Economic Warfare

10 Roy Kais, "Nasrallah: There's no need for chemical weapons, we'll strike at power stations," *Ynet*, September 3, 2012, https://www.ynet.co.il/articles/0,7340,L-4276742,00.html [Hebrew].

11 "From Tourism Destinations to Terrorism Targets: A Concrete Threat against Egypt," *Shorty* (blog), January 14, 2016, http://www.inss.org.il/he/blogs/?pauthor=55226 [Hebrew].

Defense against Broad Economic Warfare

Broad economic warfare also has a defensive aspect. A state's means of defending against such warfare include:

- Deterrence—developing a reliable response capacity and the ability to mount a counter-response;
- Active physical defense—such as the Iron Dome system—and passive defense systems, including the fortification of economic installations;
- The dispersion of infrastructure and strategic economic installations throughout the country; development of the capacity to back up systems and alternative systems, for example, in the realms of communications and energy;
- Cyber defense of the economy (see below);
- Maintenance of reserves of fuel, food, spare parts, and foreign currency in quantities greater than those necessary to meet regular needs;
- Development and maintenance of the ability to self-produce critical products, such as energy (for example, the development of Israel's natural gas fields), food, cement, and so forth;
- Diversification of sources of import in general and critical products in particular, of export destinations, and priority given to long-term contracts with reliable parties who are not influenced by the political conflict in the region;
- Designing of a plan for business continuity in states of emergency, including the development of an ability to recover and to effectively manage the economy during states of emergency, while practicing and providing guidance about this ability prior to declaring states of emergency.

The Advantages and Disadvantages of Broad Economic Warfare

The use of broad economic warfare, of course, has its advantages and its disadvantages. Its advantages include:

- The ability to apply broad economic warfare using a wide spectrum of implements and intensities, such as boycotts, sanctions, blockades, cyberattacks, and kinetic attacks, and to manage and control the campaign until its objectives are met.
- Broad economic warfare can be applied remotely and without many risks to the party exercising it, except for certain kinetic attacks.

- During wartime, broad economic warfare can exert economic pressure upon the enemy to discontinue fighting or to exact an economic price upon the enemy, in order to delay the beginning of the next war while minimizing the loss in human life.
- Broad economic warfare can also be used in campaigns between wars.
- Broad economic warfare, or the threat of its application, can also serve as a deterring factor.

The limitations and dangers of using broad economic warfare include:

- Miscalculation—Use of broad economic warfare may spark or accelerate negative processes and even lead to war. For example, in June 2018, Iran announced the acceleration of its uranium enrichment activities in response to the United States' re-imposition of sanctions against it.[12] From a historical perspective, the economic sanctions that the United States and China imposed on Japan in response to its invasion of China in 1937 resulted in a chain of undesirable outcomes: an alliance between Japan, Nazi Germany, and Italy, followed by Japan's December 1941 attack on Pearl Harbor; and in response to the attack, the United States declared war on Japan, and Japan's allies (including Nazi Germany) declared war on the United States. These developments ultimately resulted in the United States' entry into World War II.
- The population of the enemy country may come to feel hate for the party exercising the broad economic warfare, so that the economic pressure results in popular support of the regime under attack.
- Severe economic pressure could result in large-scale damage to a weak civilian population, which, in turn, could result in a humanitarian crisis and fundamental international criticism.
- Counter-reaction—The rival or enemy could develop an ability to respond using the same implements or others. The outcome could be the evolution of a war in which the assailant also sustains heavy damage.
- Broad economic warfare could result in damage to the assets or economic interests of countries that are friendly or neutral toward the assailant. An example is damage caused to an economic asset in an enemy state, which is ensured by a friendly country, or a computer attack that affects

12 Daniel Salameh and Liad Osmo, "Iran: The Construction of a Facility to Build Advanced Centrifuges Will Be Completed Next Month," *Ynet*, July 7, 2018, https://www.ynet.co.il/articles/0,7340,L-5280313,00.html [Hebrew].

unintended targets. Such incidents are liable to result in counterreactions to the party engaging in the warfare.

Broad Economic Warfare in the Cyber Era

The following is a survey of the overlap between broad economic warfare and the cybersphere.[13] The information and technological revolution that affects the economy and society continues unabated, as the development of computer clouds, big data, augmented reality, artificial intelligence, autonomous vehicles, and "the internet of things" accelerate the reciprocal relations between the economic and social on the one hand, and the cybersphere—which has become increasingly significant in the lives of individuals, organizations, countries, and the world economy—on the other hand.

Today the majority of activity of the economic sector, such as banking and finance, occurs in cyberspace while this sector minimizes its non-digital activity. Although the economic sector is real and tangible, encompassing customers, a work force, land, raw materials, and the products of the metal, building, and food industries (to name a few), all of these are represented in the cybersphere, which documents and links them together, so that a cyberattack affects the entire sector. Another important phenomenon is the globalization of trade and capital markets, which rely on the interlinked internet and cyber systems.

In cyber warfare, the cybersphere is used to damage different enemy targets, with the primary aim of achieving political and military objectives. Cyber warfare may be waged in conjunction with conventional warfare or it can be used on its own. It can be used between wars or during wars, and it can be both defensive and offensive in character. Broad economic warfare uses the cybersphere both to attack economic targets belonging to the enemy, and to defend the country's economic assets and cyber infrastructure, or those connected to the cybersphere itself—for example, factories, power stations, and airports—against enemy cyberattacks.

13 The conceptual expansion of "economic warfare" into "broad economic warfare" also facilitates discussion of powerful cyberattacks that are difficult to include under the standard definition of "economic warfare."

Cyberattacks on the Economy

A cyberattack is an attack against cyber systems that constitute digital infrastructure (for example, organizational software and databases), or an attack carried out by means of cyber (without damaging it) against computer embedded systems operating outside the cybersphere, such as power stations, control towers, traffic light control stations, and so forth. The uniquely offensive aspect of cyber warfare lies in its ability to carry out actions remotely, via cyber, without being directly exposed.[14] In doing so, the attacker does not endanger itself and can follow a policy of ambiguousness (including the avoidance to take responsibility). At times, an attack is not immediately discernible on the surface, and it takes time to be identified (for example, during the disruption of databases).[15]

Cyberattacks against the enemy economy can be carried out in various ways and can be executed at low or high intensity in combination with sanctions or kinetic attacks (using military force). In wartime, cyber has an advantage over kinetic attacks in attacking financial institutions. Cyberattacks can sometimes be used as a substitute for kinetic weapons.

Cyberattacks can serve as an additional means by which terrorist organizations disrupt the way of life in the states they are targeting, particularly given that they can be carried out from anywhere in the world, and not only from close range. Nonetheless, powerful cyberattacks carried out by terrorist groups are still uncommon, although they are expected to increase once terrorist organizations acquire the abilities that enable them to carry out high-intensity cyberattacks with visible results. Furthermore, cyberattacks help—or could help—terrorist organizations acquire funds to pay for their activities. In addition, cyber enables terrorist organizations such as Hezbollah and Hamas to carry out intelligence gathering missions[16] and psychological warfare.

Countries that seek to acquire offensive capabilities have established military cyber organizations. For example, in June 2009 the United States established the US Cyber Command, and in May 2018 this body received

14 These interactions are referred to as non-face-to-face business relationships or transactions.

15 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum no. 117 (Tel Aviv: Institute for National Security Studies, 2012).

16 Tal Shahaf, "Hamas's Next Battle Arena: Cyber," *Globes*, April 18, 2018 [Hebrew].

the status of a Unified Combatant Command.[17] Upon its establishment, it announced that the offensive cyber activity against the enemy was meant to create five effects (the five Ds): (1) deny the enemy or rival the ability to operate in cyber; (2) degrade the status of the enemy or rival; (3) disrupt the activity of its systems (4) deceive; and (5) destroy its abilities. These five effects are also relevant to cyber-based broad economic warfare.

Cyber is a platform in which many economic actions are taken, and through these actions, it is possible to intensify economic warfare, such as in the increased enforcement of economic sanctions. Cyber also enables control of the economic realm, for example, by preventing an enemy country from accessing trade and financial systems; blocking the movement of money; preventing the conveyance of trade instructions; implementing information gathering actions and exposing companies that are violating sanctions; freezing and supervising bank accounts; controlling foreign currency across borders through the reports of financial institutions located outside the enemy country; and controlling trade by authenticating data with suppliers outside the enemy country.

Economics by nature is highly sensitive to information, and a significant share of economic systems is based on the public's confidence in the economy and its institutions, such as banks, the national currency, and the systems overseeing the capital markets. Cyber-based broad economic warfare can serve to undermine confidence in the economic systems, including by disseminating relevant information. Still, it is no simple matter to be successful in information warfare of this kind, as cyber also enables the attacked to respond quickly and to refute rumors against it.

Cyberattacks against regime institutions, such as by blocking public access to them, are liable to impair governance and damage the economy and state's income. This is because cyber is a means of establishing a connection between businesses and citizens on the one hand, and government on the other, which has increasingly become a practical—and not only informative—connection, as in the case of paying taxes and fees through websites of governing institutions. Cyber penetration and the gathering of technological and industrial intelligence also enable attackers to acquire a corporation's

17 Ami Rojkes Dombe, "United States Cyber Command Awarded Status of Combatant Command," *IsraelDefense*, May 6, 2018, http://www.israeldefense.co.il/he/node/34080 [Hebrew].

intellectual property. Such actions, when carried out on a significant scale, can change the strategic balance between global corporations, as well as between countries. For example, the United States claims that China carries out such actions in its territory.[18]

Cyberattacks can be managed at a high level of intensity with the aim of disrupting trade, production, and financial activities of the attacked state, such as by damaging databases of trade systems, logistical depots, budgets, and so forth. Such actions are located on the border of "soft" warfare and can also reach higher levels of warfare (depending on the intensity and the scope of the damage). Cyberattacks can be carried out at a higher intensity as part of "hard" warfare. Such attacks are intended to impair the operation of infrastructure and economic systems (electricity, water, banking, transportation, communication), to the point of fundamentally disrupting daily life and the functioning of the enemy state. The ability to remotely damage the functioning of economic systems, without crossing territorial borders and without using military force, is a unique advantage of cyber. At the same time, certain offensive actions carried out in cyber can be disastrous for the country attacked, including loss in human life and damage to essential infrastructure. Such cases are similar to a kinetic attack, and the attacked country's response is liable to be commensurate.

Among the countries that employ cyber to attack economic targets is Iran. In August 2012, Iran was attributed as having carried out a cyberattack against the Saudi national oil company Aramco, using the Shamoon virus. The virus infected some 30,000 computers and impaired the functioning of the company.[19] In 2013, it was reported that Iranian hackers carried out a series of cyberattacks against American targets, including large banks and energy companies operating in the Persian Gulf, but did not result in any significant damage.[20] Another attack using the Shamoon virus, also attributed to Iran, was executed at the end of 2016 against the central bank of Saudi

18 "The United States Accuses China of Stealing $400 Billion in Business Information," *The Marker*, February 17, 2012, https://www.themarker.com/wallstreet/1.1644216?= [Hebrew].

19 Amos Harel, "Assessment: Iran is behind the Cyberattack on the Oil Companies in the Persian Gulf," *Haaretz*, September 11, 2012, http://www.haaretz.co.il/news/world/1.1821619 [Hebrew].

20 "Report: Iran is Conducting an Online Attack against the United States," *Ynet*, October 13, 2013, https://www.ynet.co.il/articles/0,7340,L-4291493,00.html [Hebrew].

Arabia and other state bodies in the kingdom.[21] According to assessments, Iran could respond to US-imposed sanctions with a massive cyberattack.[22] This, however, would expose Iran to the risk of severe retaliation. North Korea, which is also currently subject to sanctions, established a cyberattack apparatus and carries out such attacks primarily against South Korea and Western countries.[23] The above examples indicate that cyber warfare serves as a means of response for countries that are subject to sanctions.

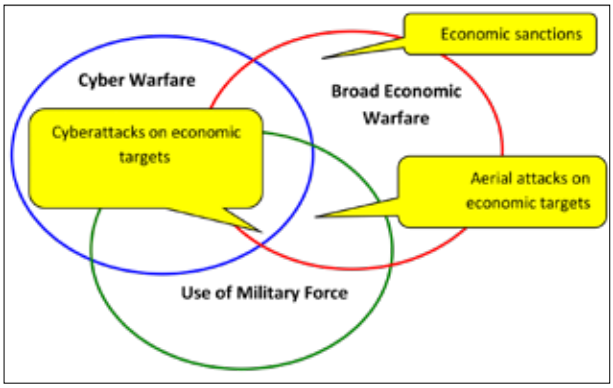

Figure 2. Broad Economic Warfare and Cyber Warfare (Examples)

Defense against Cyberattacks

The Cyber Threat Against the Economy

The state and global economy depends on information systems, databases, communications, and automatization, and their dependence on cyber continues to increase. Today, certain branches of the economy, such as communications and banking, are already deeply entrenched in the cybersphere, and others,

21 "Iranian Hackers Broke into Computers of the Saudi Central Bank," *The Marker*, December 3, 2016, https://www.themarker.com/wallstreet/1.3140741 [Hebrew].

22 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

23 David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

such as power stations, factories, and transportation operate by means of computer and cyber-embedded systems.

The doomsday scenario of a cyberattack on the economy includes a situation in which banks close; stock market trading ceases; and the operation of power stations, water systems, and transportation enterprises and systems are severely disrupted. According to this scenario, air traffic will cease at airports; factories and offices will close their doors; and foreign trade will come to a standstill. As a result, citizens will have difficulty performing basic actions, such as withdrawing money, receiving their salaries via banks, filling up their gas tanks, buying food at the grocery store, moving from place to place, finding employment, and communicating with government institutions. The government will have difficulty managing the economy and collecting taxes, and all the activity of the economy will grind to a halt. In practice, such broad-scale damage is not necessary to stop the processes of the economy, as striking at a few of its sensitive links is sufficient. So far, however, there has not yet been a cyber event on the doomsday scale, possibly due to the limited abilities of many cyber actors given the defense mechanisms that have been set up by different countries (there is a big difference between a cyber strike on one target or another, and systemic cyber damage to the economy); caution on the part of cyber powers to avoid premature exposure of cyber weapons; fear of countermeasures; and the desire to avoid sparking a cyber arms race and a global cyberwar.[24]

To complete the picture, the most dramatic cyber events in recent years pertaining to national security have occurred in the field of governance in democratic states. For example, the United States maintains that Russia conducted a cyberattack in order to influence the results of the 2016 US presidential election, which has been perceived as a concrete threat to the American democracy. Russia was also accused of trying to interfere in the French presidential elections in 2017 using a similar method—the dissemination on social media of sensitive information against one of the candidates, which it acquired by hacking the computers connected to the

24 Gadi Evron and Boaz Dolev, "War Games: Why the United States is Not Conducting a Cyberattack against North Korea," *Ynet*, September 19, 2017, https://www.ynet.co.il/articles/0,7340,L-5017828,00.html [Hebrew].

candidate.[25] On the other hand, cyber capabilities enabled Turkey's President Recep Erdoğan to thwart a military coup attempt staged against him in July 2016, when he used a cellular application broadcasted to the television and called on his supporters to violate the curfew imposed by the military and to take to the streets.

The state gives preference in terms of cyber defense to its state critical infrastructure (SCI). In Israel, SCI includes electricity infrastructure, water, natural gas, trains, the airport authority, refineries, the electricity production chain and its conduction, government offices, and hospitals. It encompasses twenty-six critical infrastructures that receive instructions directly from the National Cyber Directorate.[26]

The financial sector (banks, credit companies, the credit card clearing system, the capital market, insurance, and pension funds) is particularly sensitive to cyberattacks, due to its critical role in mediating economic and social activities. Unlike heavy industry, the financial sector is more vulnerable to cyberattacks than kinetic attacks. The financial system is based on cyber, sensitive to public confidence, and critical for state functioning. An example of a cyberattack on the financial system was the theft of $81 million in February 2016, when hackers (possibly from North Korea) succeeded in moving funds to the Philippines from the Central Bank in Bangladesh that were held in accounts in the Federal Bank in New York.[27] A similar case of monetary theft took place at a Vietnamese bank at the beginning of 2016. During this event, hackers penetrated the SWIFT system, which is considered to be the most secure interbank payment system in the world.[28] These examples reflect capabilities that can be exercised to a greater extent within the framework of broad economic warfare.

---

25 David Siman-Tov, Gabi Siboni, and Gabrielle Arelle "Cyber Threats to Democratic Processes," *Cyber, Intelligence, and Security* 1, no. 3 (December 2017): 51–63, http://www.inss.org.il/wp-content/uploads/2018/01/CyberENG1.3_6-53-65.pdf.

26 Dan Arkin, "Well Prepared for Threats," *IsraelDefense*, May 24, 2018, http://www.israeldefense.co.il/he/node/34321 [Hebrew].

27 "Operation Lazarus: This is How North Korea Steals Money from Banks in the West through Cyberattack," *Nana*10, April 5, 2017, http://media.nana10.co.il/Article/?ArticleID=1240370 [Hebrew].

28 "Cyberattack on Global Banking: Hackers Again Break into the World's Most Secure Payment System," *The Marker*, May 13, 2016, https://www.themarker.com/wallstreet/1.2942637 [Hebrew].

Other companies in the economy that are sensitive to cyberattacks include those dealing with infrastructure, defense, internet trading, and organizations that make use of sensitive information (law firms, stores of intellectual property, commercial secrets, medical secrets, and so forth). Recent years have witnessed an increasing awareness that organizations' supply chains—the bodies that supply these organizations with intermediate products and with services—constitute an entry point for many of the cyberattacks. This means that defense is required not only of essential targets in the economy but also of the peripheral, surrounding ones as well.

Company employees, including those within the defense industries that deal with the cybersphere, also pose a cyber threat. One example is the serious defense affair that was exposed in July 2018, when an employee of the offensive cyber company NSO was arrested on suspicion that he stole cyber weapons from the company (Pegasus spyware) and attempted to sell them for $5 million. The employee's attempt was thwarted after the "potential buyer" informed the company. This event reflects the need for the state to also supervise what goes on in companies that work in the cybersphere.[29]

Most of the economic damage in the cybersphere up to present has not been caused by broad economic damage by states or organizations but rather by criminals whose primary motivation is financial. Nonetheless, we must assume that everything the criminal sector can do in the cybersphere can also be done by states, which have the capacity to cause even more damage should they choose to wage massive cyber warfare. The 2010 exposure of cyberattacks using the Stuxnet worm that destroyed Iranian centrifuges for the enrichment of uranium illustrates such a powerful state ability.[30] These cyberattacks made it clear to the world that the threat they posed also includes physical damage to industrial plants, infrastructure, and transportation—all of which are equipped with computerized command and control systems—and is not limited solely to damage to databases in the cybersphere.

---

29 Ela Levi-Weinrib and Tal Shahaf, "Permitted for Publication: NSO and One of the Most Serious Cyber Affairs in the History of Israel," *Globes*, July 5, 2018, https://www.globes.co.il/news/article.aspx?did=100124461 [Hebrew].

30 "The Iran File Has Been Opened: Cyber War," Israel Channel 2: *Uvda*, November 2, 2012, https://www.mako.co.il/tv-ilana_dayan/specials/Article-a996bba5fccba31006.htm [Hebrew].

The Response to the Threat

Severe damage to the state's cybersphere should be considered a national security problem. Cyber defense in its economic context involves an array of actions both inside and outside the cybersphere, aimed at defending the state economy against attacks that make use of cyber, both in the cybersphere and in other areas. Cyber defense must be implemented to protect against other states, enemy organizations, crime groups, and malicious actors, as well as to recover from mishaps.

The primary difference between the economic warfare of states that use cyber and criminal activities in this realm is that cyber criminals' motivation is typically criminal and financial (such as the theft of money, commercial secrets, or intellectual property; extortion; collecting ransom).[31] At the same time, however, in some cases, states have related to large-scale cybercrime and even to the unusual economic activities of bodies operating for the sake of profit as threats to their national security.[32]

Whereas border defense and defense of the home front against missiles are the responsibility of the army, defense of the economy's cyber assets—in Israel and around the world—depends primarily upon security services, strategic products of the private sector, and the resources of the sector. A diverse industry of companies produces, markets, and provides support for cyber defense systems.

The need of the private sector—and not of the state— to defend itself against cyber theft of finances, intellectual property, and commercial and technological secrets, as well as cyberattacks motivated by ideological or psychological reasons (ego, vandalism, and so forth) has been the force in

31 Alan Blinder and Nicole Perlroth, "Atlanta Hobbled by Major Cyberattack that Mayor Calls 'a Hostage Situation'," *New York Times*, March 28, 2018, https://www.seattletimes.com/nation-world/atlanta-hobbled-by-major-cyberattack-that-mayor-calls-a-hostage-situation/.

32 For example, at the beginning of 2010, in the midst of the financial crisis in Europe, speculators were marked as "economic terrorists." At the time, the German finance minister said that Germany would consider instructing its intelligence agencies to begin monitoring the organization and activity of speculative investors in order to protect the euro. In addition, the Spanish newspaper *El Pais* reported that Spain's secret service had initiated an investigation of "attacks" on the state by speculators.

developing a cyber defense industry in the local and global economy.[33] The primary role of government security entities in defending the economy lies in its instruction and supervision of prominent bodies of considerable importance. The state is engaged primarily in defending its institutions and instructing organizations that are classified as SCI. At most, the economy and population have the ability to contact the national emergency hotline (CERT) and to access the guide for cyber defense.

Cyber technology is characterized by a rapid pace of change, making it difficult to anticipate how it will look in just another few years. As a result, it is difficult to draw up multi-year programs in the sphere of cyber defense.[34] Rapid change also means high costs of technological depreciation, as things that are installed today will not necessarily be relevant in a few years' time and new versions of software will need to be updated regularly, increasing the dependence on suppliers of technology.

In most cyberattacks, it is difficult to identify the attacker (who takes precautions to conceal his or her identity and to evade detection) and the number of attackers involved; thus, organizations and companies are obligated to adopt broad cyber defense strategies aimed not at specific attackers but rather at various kinds of attacks coming from different sources with increasing level of difficulty, all in order to address the rapid technological developments in the field. Initially, peripheral defense systems were developed, emphasizing defense against remote penetration and the removal of viruses that penetrated the system. However, over the past decade, systems have been developed to halt or deter unauthorized and possibly hostile activity undertaken by someone who physically can penetrate the organization (close contact penetration), including an employee or supplier. Today, physical defense systems, security officers, and the use of manpower selection systems in human resource departments also play important roles in the cyber defense system.

Over the years, the state has made defending infrastructure and the financial sector against cyberattacks a regulatory requirement. In this context, bodies

33 Gabi Siboni and Hadas Klein, "Developing Organizational Capabilities to Manage Cyber Crises," *Cyber, Intelligence, and Security* 2, no. 1 (May 2018): 21–38, http://www.inss.org.il/wp-content/uploads/2018/05/Developing-Organizational-Capabilities-to-Manage-Cyber-Crises.pdf.

34 "From Zion the Cyber Will Come Forth," Product of Israel: A Special Insert for Independence Day, *Haaretz*, April 2018 [Hebrew].

have also been established to engage in cyber defense on a national level. In Israel, for example, a national authority for information security began operating within the General Security Service (GSS) in 2002; in 2011, the National Cyber Directorate was established; in 2015, the National Authority for Cyber Defense was created;[35] and at the end of 2017, the government decided to form a national cyber directorate in the Prime Minister's office, as a merger of the National Cyber Directorate with the National Authority for Cyber Defense.[36] Despite all these measures, Israel still has a long way to go until it achieves full defense of its national cybersphere. As a vision for the future, we can expect the state to assume more practical responsibility in defending the cybersphere of the entire economy and population. Just as the state provides clean water and a steady flow of electricity to both businesses and residences, it should ensure that computer communications are stable and untainted by malware.

Given the above, it is extremely important to integrate the government and the private sectors within the realm of cyber defense. The state needs to integrate the private sector into the national cyber defense activity, both as a major consumer and as a partner in the defense system.[37] One example is the establishment in January 2017 of a banking center for cyber defense in Israel, which was a joint initiative of the National Cyber Defense Authority, the Finance Ministry, Banking Supervision, the banking corporations, and the credit card companies.[38] Israel has an advantage in this area due to its relatively small number of banks, close government supervision, and high levels of cyber capability; still, a minority of banks may be disadvantaged from the perspective of risk diversification.

The fact that cyberspace does not have territorial borders requires international cooperative efforts for national cyber defense. Indeed, at a

35 Ami Rojkes Dombe, "The Cyber Authority Will Replace the GSS in Overseeing Information Security in Banks," *IsraelDefense*, May 9, 2016 [Hebrew].

36 See the website of the National Cyber Directorate at https://www.gov.il/he/Departments/about/newabout [Hebrew].

37 Shmuel Even, "The Strategy for Integrating the Private Sector into National Cyber Defense in Israel," *Military and Strategic Affairs* 7, no. 2 (September 2015): 103–124, http://www.inss.org.il/wp-content/uploads/systemfiles/MASA7-2Eng%20Final_Even.pdf.

38 "A Cyber Banking Center Was Established and Started to Operate in January," *Read it Now*, March 20, 2017, https://www.readitnow.co.il/news [Hebrew].

NATO summit held in July 2018, the leaders of the member states also agreed to increase their countries' preparedness against cyberattacks.[39] In the Israeli context, GSS Director Nadav Argaman maintains that "the State of Israel is currently one of the world's leading cyber power, and this includes the security system and the Israeli intelligence community. We, of course, cooperate with intelligence services and security systems from around the world. As an organization, we have quite a significant cyber capability, both for defense and for offense. We, of course, cooperate with the overall Israeli security system and do nothing alone. We have extremely broad capabilities."[40]

An example of international cooperation in the financial sphere is the Financial Action Task Force (FATF),[41] which was established in 1989 to develop and promote a policy to fight money laundering and the funding of terrorism and weapons of mass destruction. Despite their differences, these areas all deal with finances from sources that are intended to be hidden, and the means of dealing with them are similar. This organization has pointed out that one of the risks in the cyber era is the ability to conduct illegal transactions and to use unlawful funds in cyber, without the direct (face-to-face) exposure of the person performing the action. The FATF also issued a list of criteria according to which states that are not members of its framework will be checked, and if it is decided that they do not meet the criteria, they could be placed on a blacklist that allows them to be subjected to heavy sanctions.

The risk posed by transferring unlawful funds has increased in recent years along with the emergence of the use of Bitcoin, Etherium, and other virtual currencies that facilitate transactions outside the institutionalized state and global financial system. The evolution of means of payment and financial systems located outside the realms of state control could have far-reaching consequences, such the mobilizing of funds by terrorist groups and subversive organizations and the funding of terrorist activities; the bypassing of sanctions; secret payments for sensitive and prohibited technologies and materials (such as non-conventional weapons, surface-to-surface missiles, cyber capabilities); undermining of the established

39 "NATO Has Survived Trump, For Now," *Haaretz*, July 15, 2018 [Hebrew].

40 Itay Blumenthal, "GSS Head: This Year We Thwarted Cyber Attacks from around the World," *Ynet*, January 30, 2018, https://www.ynet.co.il/articles/0,7340,L-5078254,00.html [Hebrew].

41 http://www.fatf-gafi.org/home.

financial system; impairment of tax collection; cybercrimes and ransom; money laundering; the payment of bribes; and damage to public funds. Different countries take various approaches toward these currencies, but the international system has yet to make a joint decision on the issue. The heads of the financial system in the West do not regard virtual currency as an imminent threat, given the phenomenon's limited scope in comparison to the world capital market. If the phenomenon of digital currencies spreads, it will be necessary to take legislative and enforcement measures on the state level and to reach international agreements that may ultimately be significant to solving the problem.[42]

The need for global cooperation in cyber defense is clear. The International Telecommunications Union is working to promote global agreement regarding defense of the cybersphere. There have also been attempts to formulate an international convention regarding cyber defense, similar to those conventions limiting the proliferation of chemical and biological weapons. The chances are low, however, as it would require reliable oversight and a validation mechanism, which is difficult to implement in the cybersphere.[43] The United States apparently is also concerned that such a convention would limit its abilities and not significantly contribute to its defense, which further decreases the chance of achieving agreement on an effective convention in this realm.

Conclusion

The first part of this article presented the concept of broad economic warfare, which has a wider scope than economic warfare according to the standard definition. The second part of the article discussed cyber warfare as an element of broad economic warfare. Broad economic warfare enables a systemic discussion of a variety of actions that can be conducted against an enemy's economy using diverse tools, including economic, diplomatic, cognitive, kinetic, and cyber means. The aim of these actions is to weaken the enemy's economy, primarily in order to achieve political and military goals. Conducting broad economic warfare in the cyber era depends upon

42 Shmuel Even, "Internet Currencies and National Security," *INSS Insight*, no. 1003, December 28, 2017.

43 Cameron S. Brown and David Friedman, "A Cyber Warfare Convention? Lessons from the Conventions on Chemical and Biological Weapons," in *Arms Control and National Security: New Horizons*, Memorandum no. 135, ed. Emily B. Landau and Anat Kurz (Tel Aviv: Institute for National Security Studies, 2014).

the development of offensive and defensive capabilities alike. Offensive abilities are imperative for the sake of defense, deterrence, and retaliation, whereas defensive cyber capabilities are also essential in offensive situations, in order to withstand a counterattack.

The cyber era has changed the realm of broad economic warfare. From an offensive perspective, it is possible to strike at the enemy's economy during wartime and between wars, using "soft" cyber warfare and high-intensity cyberattacks that may be preferable to kinetic attacks, which are frequently accompanied by human casualties. From a defensive perspective, the increasing dependence on the cybersphere intensifies the cyber threats that are posed to state economies and therefore states require significant efforts and heavy investments to defend the economy, in addition to cooperative efforts within the economy, between the private economy and the government, and among states in the global system.

Although extreme scenarios of cyberattacks on state economies have thus far not materialized, the pace of building defenses for the state cyber system must adapt to the rapidly accelerating establishment of the economy within the cybersphere.