Critical Infrastructures and their Interdependence in a Cyber Attack – The Case of the U.S.

Harel Menashri and Gil Baram

The growing use of information technology, monitoring, and control through computerized control systems, together with the increasing dependence of the free market on products and services supplied through infrastructure (for example, electric power), have increased interdependency between infrastructures. Consequently, an attack on critical infrastructure is liable to have a decisive effect on the functioning of other infrastructures. The interdependence between infrastructures requires those involved in planning a cyber-attack as well as those involved in defending from such attacks to adjust to this reality and prepare accordingly. The article describes the existing models for analyzing interdependence between infrastructures, proposes an analytical framework for describing the interdependence and examines the possibilities at the United States' disposal should it decide to engage in a cyber-attack.

Key Words: critical infrastructure, interdependence, cyber-attack

Since the September 11, 2001 terrorist attacks, the U.S. administration has adopted a series of actions in order to improve security issues, including cyber security. As early as November 2002, President George Bush signed National Security Presidential Directive No. 16, directing government agencies, headed by the Department of Homeland Security (DHS), to develop

Dr. Harel Menashri is a fellow at the International Institute for Counter-Terrorism at the Herzliya Interdisciplinary Center.
Gil Baram is a doctoral candidate in the program for outstanding students in the Political Science Department at Tel Aviv University, and a researcher at the Yuval Ne'eman Workshop for Science, Technology and Security.

national guidelines determining when and under what circumstances the U.S. will be able to carry out cyber-attacks from its territory.[1] In February 2003, the White House published a document called "The National Strategy to Secure Cyberspace," portraying cyber security as a matter under the responsibility of the DHS. The purpose of the document was to provide "a framework for protecting the infrastructures that are essential to our economy, security, and way of life." The document contained a broad range of actions designed to protect the U.S. national security through the defense of its key critical infrastructures. The goal of this strategy was to create a working framework that would, for the first time, define priorities and instruct the various governmental authorities how to act in order to strengthen their cyber defense.[2]

Widespread activity in this sphere also took place during President Obama's term in office, with an emphasis on the importance of the cyber threat in the context of the publication of the National Security Strategy in May 2010, as well as publication of the International Strategy for Cyberspace in May 2011, which lay the foundation for clear methods of action in dealing with the cyber threat. This was reflected in a Pentagon statement according to which when warranted, the United States will respond to hostile acts in cyberspace as it would to any other threat to the country.[3] In November 2014, the director of the National Security Agency (NSA) issued a warning about Chinese and "two or three other countries'" ability to damage critical infrastructure in the U.S., including electricity, aviation, and financial systems, through cyber-attacks.[4] In January 2015 President Obama asked Congress to pass legislation on the subject of facing the growing cyber threat.[5] These official statements and others indicate that cyber security and defense of critical national infrastructures have been on the U.S. decision-makers' agenda for almost two decades, and they are of considerable importance to the American administration.

The interdependence between infrastructures requires those planning a cyber-attack to consider the connections between the infrastructures that they plan to attack and other infrastructures, including those in the target country, in the attackers' country, and in other countries in order to avoid damage that will affect the infrastructure in their own country, as well as avoid damage to other infrastructures which is liable to be considered a war crime. The parties defending infrastructures must study and map the connections and interdependency between the various infrastructures,

provide for redundancy, and prevent a domino effect in the event of damage to one of them.

The purpose of this article is to propose a general framework for describing the interdependence between infrastructures, and to examine the possibilities at the U.S.'s disposal in conducting a cyber-attack. The article is constructed as follows: first, the existing models for analyzing states of interdependency between infrastructures are presented and described. It should be noted that even though these models are not new, they are very relevant to the present time, because almost no changes have occurred in the development and operative characteristics of most of the infrastructures over the past decade, a fact that constitutes a significant weak point, and makes them an easier target for cyber-attacks. Next, the article analyzes the mutual interdependency between infrastructures in the case of the U.S., and assesses the consequences that decision-makers in the U.S. must take into account, in addition to considerations such as beginning a campaign that will jeopardize American infrastructures.

An Attack on Co-Dependent Infrastructures

There is a link between the infrastructures in industrialized countries like the U.S. and the infrastructures in other countries, and at times they are dependent upon each other. The global economy and trade relations between countries rely on electronic communications that facilitate ties, commercial transactions, and transmission of information and knowledge around the world at almost the speed of light. In many countries, technological progress – mainly in the field of communications – enables giant international corporations to operate and maintain this infrastructure. American corporations also invest resources in the infrastructures and economies of other countries. The global economy depends on a constant supply of energy resources. For example, the Chinese economy depends on a supply of energy resources from the Persian Gulf.

The introduction of critical infrastructures into all industrial sectors (such as water, energy, transportation, and the like) is accompanied by major long-term investments. Construction of these infrastructures takes many years, and therefore the management, monitoring, and control system for these infrastructures (Supervisory Control and Data Acquisition, SCADA), which are based on programmed industrial controllers, are infrequently revised, unlike the prevailing frenetic and rapid time spans in the current cyber world. Accordingly, an assessment of the durability of infrastructure

systems is also based on conservative models which, despite the time that has passed since they were developed, are still valid and relevant.

According to the model set forth by Steven Rinaldi,[6] when countries share common infrastructures, for example electricity, water, and gas, an attack on the infrastructure of one country is liable to affect the infrastructure of the other country. Clearly, the U.S. infrastructures and economy are liable to suffer devastating damage if the infrastructure and economies of other countries linked to them are attacked.

Together with the interdependency between countries, there is also mutual interdependence between infrastructures within the same country. An attack on one infrastructure is liable to cause a chain reaction or domino effect, in which infrastructures are damaged one after another. For example:

1. Infrastructure that produces electricity depends on a resource supplied through other infrastructure, such as oil or gas. An attack on the oil or gas infrastructure will affect the electrical infrastructure.
2. An attack on financial infrastructures, such as a stock exchange and banks, is liable to damage other infrastructures that require a flow of cash for their activity. Obviously, other scenarios of damage to public order due to economic problems are also possible.
3. An attack on the U.S. railway infrastructure is liable to have a severe effect on trade in the U.S. and its economy, and could cause food shortages in various regions throughout the country within a few days.
4. An attack on power plants or the transforming of electricity during peak periods is liable to cause a chain reaction in which additional power plants stop functioning. Such an event occurred in the U.S. in August 2003, when an operational malfunction in a transforming plant resulting from negligence caused a crash in electricity production and supply systems. This was the worst power blackout in the history of North America – residents of the northeastern U.S. and Canada were cut off from the electricity grid for many hours and even days.[7]
5. An attack on electrical infrastructure is liable to have an immediate effect on other national and municipal infrastructures: hospitals, industrial production, and damage to communications and transportation systems, mainly on land, but also certain air transportation systems.
6. An attack on the traffic system in a busy traffic lane will cause a transportation chain reaction that will affect other systems whose activity depends on transportation infrastructures.

In the process of planning an attack on an enemy's critical infrastructure, the attacker must consider precisely how the target infrastructure is linked to other infrastructures, and how these infrastructures depend on each other. It is sometimes possible to consider the possibility of attacking the target infrastructure by means of an attack on other infrastructure connected to it: a weak point may be found in the systems of the connected infrastructure that will make it easier and more convenient to attack.

The theoretical methodology used to assess the interdependence between critical infrastructures is displayed in Figure 1 below, taken from a study by Gillette, Fisher, Peerenboom, and Whitfield.[8] The diagram demonstrates the links and interdependence between the critical infrastructures, with electrical infrastructure in the center linked to all the others, and all of them dependent on its proper operation.

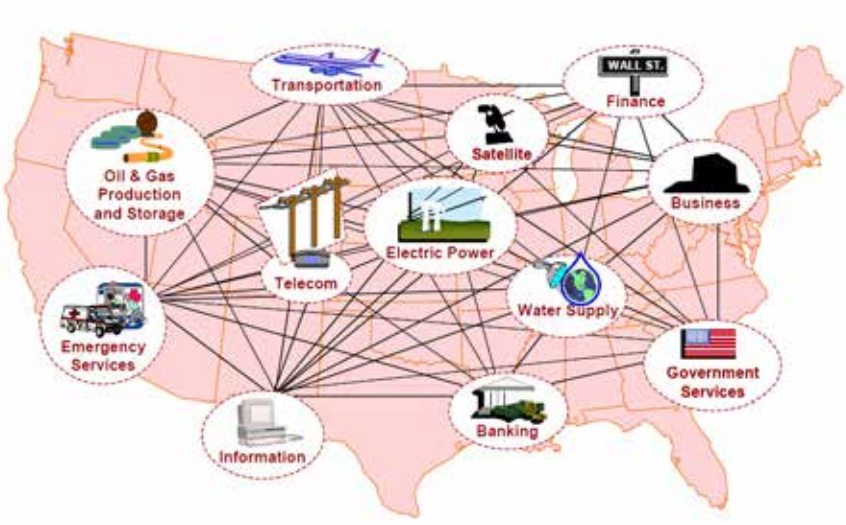


Figure 1: Critical Linked and Interdependent Infrastructures in the United States

Source: Gillette, J., Fisher, R., Peerenboom, J. and Whitfield, R, *Analyzing Water/ Wastewater Infrastructure Interdependencies* (Lemont, Illinois: Infrastructure Assurance Center – ANL, Argonne National Laboratory, 2006).

Addressing Interdependence between Infrastructures

The issue of mutual interdependence between critical infrastructures in the U.S. is mentioned for the first time in 1998, in Presidential Decision Directive No. 63, which deals with protection of infrastructure.[9] Two events influenced the publication of this directive: the attack on the government building in Oklahoma on April 19, 1995 and the activity of the scientific task team on the subject of information warfare in 1996.

Presidential Decision Directive No. 63 stated, for the first time, that the national and economic security of the American people depended on critical infrastructures and the information systems supporting their proper operation. In order to ensure their reliability and protection, committees were established for every infrastructure sector, while the appropriate federal authority was instructed to investigate problems relevant to the sector. The activity of these committees focused on protecting the information systems against hostile penetration, i.e. computer attacks, liable to cause a failure in the essential infrastructures.

Essential infrastructures can be roughly divided into two main categories:

1. Infrastructures whose activity relies solely on information technology (IT), referring to most financial infrastructures;
2. Infrastructures operating through SCADA systems. These special control, monitoring, and management systems are typical of critical national infrastructures, such as electricity, water, gas, fuel, communications, and transportation. The information in these systems is sent from the controllers deployed in the field to the control center, and from there to the operational systems in real time. The systems use sensors providing real-time information on their status, used for controlling and implementing operational changes. For example, in a pipeline transporting material from a container to a facility that uses the material, the sensors provide a real-time status of the amount and volume of material in every part of the system.

One suitable model for describing the behavior of the essential infrastructures and the interdependence between them is based on the definition of infrastructure systems as Complex Adaptive Systems (CAS). These systems are complex, because they are diverse, and contain a large number of interlinked components. They are adaptable, because the capabilities of the components and their decision rules change over time in response to information from other components, and to external intervention. The term "CAS" was coined in 1994 at the interdisciplinary

Santa Fe Institute (SFI), by John H. Holland, physicist Murray Gell-Mann, and others in 1994. Additional examples of complex adaptive systems are the stock market, insect and ant colonies, climate systems, the human brain, and the immune system.

A General Framework for Describing the Mutual Interdependence between Infrastructures

In 2001, Rinaldi, then Chief of the Modernization and Technology Issues Branch, United State Air Force Quadrennial Defense Review Office, proposed a general framework for describing the mutual interdependence between infrastructures. In a joint study with other researchers, CAS systems were identified, and six spheres of reference were presented, according to which data could be provided concerning the mutual interdependence between infrastructures (see Table no. 1). The subject presented in the document has constituted the basis for theoretical and applied research in this field ever since.[10]

Table 1: Dimensions for Describing Infrastructure Interdependencies
(Rinaldi et al., 2001)

Types of Interdependencies	Type of Failure	Infrastructure Characteristics
· Physical Interdependency · Geographic Interdependency · Cyber Interdependency · Logical Interdependency	· Common cause · Escalating · Cascading	· Spatial (Geographic) · Temporal range · Operational factors · Organizational considerations
State of Operation (of the Infrastructure)	Infrastructure Environment	Coupling and Responsive Behavior
· Normal · Stressed/Disrupted · Repair/ Restoration	· Public policy · Legislation and regulation · Business-economic factors · Public health and safety · Political and social factors · Technology and Security	· Power of the coupling: · Tight/loose · Order of the coupling: Direct/indirect · Complexity of the coupling: Linear/complex

According to the document, the first sphere of reference that can mark mutual interdependence between infrastructures is the type of dependence. Mutual interdependence is defined as a bi-directional link between infrastructures, through which the state of each of the infrastructures is affected by the state of the other. The bi-directional characteristic is likely to be multi-channel, meaning that one infrastructure is dependent on a second infrastructure in a given channel, while the second is dependent on the first in a different channel. The interdependence between infrastructures is defined as a uni-directional link when the state of one of the infrastructures affects the state of the other infrastructure, but the second does not necessarily affect the first; for example, a communications system depends on the electrical system for the supply of electricity to the activity of its components, but the electrical infrastructure may not be dependent on the activity of the communications system.

There are four distinguishable types of interdependencies:

1. *Physical*. Two infrastructures are physically dependent when each depends on a physical product of the other. In this situation, a physical product from one infrastructure is a physical input for the other. For instance, a coal-powered power plant provides power for a railway network that transports the coal to the power station.
2. *Geographical*. Infrastructures are geographically dependent if a local environmental event can cause a change in their state.
3. *Cyber*. When the state of an infrastructure is conditioned upon information broadcast through the information or communications infrastructure. For example, production of electricity is conditioned, among other things, on information transmitted about the consumers' consumption of electricity.
4. *Logical*. Two infrastructures are logically dependent when the state of one infrastructure depends on the state of the other through some mechanism that is not a physical, geographical, or computer link. In principle, dependence of this type is created through decision-making processes made by the human factor, for example through political, legal, regulatory, or business measures (such as mergers).

The second sphere of reference that can indicate mutual interdependence between infrastructures is the type of failure. Three types of failure can affect mutually interdependent infrastructures:

1. *Common cause failure*. Disruption in two or more infrastructures simultaneously affected by a common cause. Example: failures in various infrastructures caused by weather damage.
2. *Escalating failure*. Failure in one infrastructure affects an independent disruption in another infrastructure. One example is the recovery time for repairing a failure in an infrastructure in which a component breaks down due to the unavailability of another infrastructure, delaying the delivery of spare parts.
3. *Cascading failure*. Disruption in one infrastructure will cause disruption in several other infrastructures. The most prominent example is the blackout in August 2003 in the U.S. and Canada, when a failure in the supply of electricity caused stoppages in communications and the supply of water, which in turn brought air traffic and other activity to a halt.

The third sphere of reference that can indicate mutual interdependence between infrastructures is the infrastructure characteristics. According to the above table, there are four distinguishable characteristics.

1. *Spatial scales*. This includes two aspects: the internal structure of the infrastructure itself, and the geographical deployment of the infrastructure.

   The internal structure of the critical infrastructure consists of several levels. A part is the smallest distinguishable component in analyzing the system; a unit is a collection of functionally linked parts, for example a generator; a sub-system is an array of units, for example a secondary cooling unit; and a system is an assembly of sub-systems, for example a power station. A complete collection of similar systems is an infrastructure: all the generators, cooling units, and power stations, together with additional parts, units, sub-systems, and systems, make up the electrical infrastructure.

   An interdependent infrastructure is the linked architecture of infrastructures and environment. The geographical deployment of the infrastructure can also exist on several levels: municipal, for example a municipal water supply; regional, such as regional electrical systems; national, including transportation systems; and international, including communications and financial systems.
2. *Temporal range*. In operating infrastructures, there is a very broad span of temporal ranges, varying from fragments of seconds (in operating electrical systems, for example) to hours (in water, gas, and traffic systems), to years (upgrading infrastructures and expanding capacity,

for example). This aspect is related to the power of the coupling (close or loose, as explained below) between infrastructure characteristic, which affects the relevance of the analysis. For example, in analyzing the course of a sudden failure in the electrical system, rapid processes, such as mutual computer interdependence, whose temporal ranges vary from seconds to hours, can be critical for an analysis. This is true mainly when SCADA systems and Energy Management Systems (EMS) are involved. Slower processes, such as transporting coal to power stations by rail (on a scale of weeks), legislating new energy laws (years), or construction of new power stations (years to decades) are irrelevant to an analysis relating to temporal ranges of a few days.

3. *Operational factors*. This component affects the response of infrastructures when they operate under stress or disturbance. The operating elements are closely related to security and risks. They include operational rules, training operators, backup systems and system redundancy, bypasses in an emergency, continuity plans, and plans for security policy, including implementation and enforcement.
4. *Organizational considerations*. This is an important factor in the behavior of an infrastructure. It includes the effects of globalization, international ownership, regulation, government ownership versus private ownership, policy and organizational motivation, and the regulatory environment. These organizational aspects are likely to prove key factors in determining the operational characteristics of infrastructures, and have marked consequences for security and avoidance of risks.

The fourth sphere of reference that can indicate mutual interdependence between infrastructures is the operational state of the infrastructure. This is a continuity of different behaviors during routine operational states, varying from states of peak activity to low activity, times of pressure, when disruptions are discovered, or when repairs and renovations are taking place. The state of activity of a unit, sub-system, or system during a failure affects the extent and duration of the disruption and the damage to the provision of the service provided by the infrastructure. For example, the effect of events during times of peak demand for electricity (or gas, water, telephony, or at times of heavy traffic) will be different than the effect of the same events occurring when consumption is low.

According to the table, the fifth sphere of reference for assessing the mutual interdependence between infrastructures is the environmental sphere. Infrastructures operate not only through input, output, and

operational states; they operate in an environment influenced by other infrastructures. The infrastructure environment is the framework in which the infrastructure owners and operators set targets, create value for systems, simulate, and analyze their activity, and make decisions that affect their structure and activity. The table mentions several groups:

1. *Public policy*. This involves federal energy policy, security policy, economic policy, policy in response to disasters, and the policy that defines the areas of jurisdiction. The decision made by the American Federal Communications Commission (FCC) not to regulate the services of Internet providers, which had a substantial impact on the design and growth of communications infrastructure,[11] can be cited as an example of such a policy.

   Decisions about government investments are another important factor in public policy, affecting the environment in which infrastructures operate. Some examples of this are federal investments in defense technologies, computer networks, and satellite communications, on the basis of which comprehensive commercial infrastructures were developed.
2. *Legislative and regulatory factors*. These are also part of public policy, but due to their great importance, they should be addressed separately. Legal and regulatory aspects directly affect the activity of infrastructures. Regulated infrastructures operate under a tighter system of constraints than infrastructures that are completely free of regulation. Laws that place legal responsibility for the disclosure of private, medical, and banking information illustrate this issue. Other laws are likely to affect the structure of infrastructures, for example legislation requiring that communications services be provided.
3. *Business-economic factors, opportunities, and risks*. These are important forces that shape the environment in which infrastructures operate. Owners make business and structural decisions affecting the characteristics of their activity according to these factors. Information technology developments, government supervision or deregulation, and mergers are three factors with a major influence on the business and economic characteristics of the infrastructures environment.
4. *Public health and safety*. Legislation and regulation aimed at protecting human life, property, and public health and safety have a direct impact on the activity of infrastructures and their interdependence. For example, environmental protection legislation in California sets stringent standards

for pollutant emissions from power stations and for reducing air pollution and other health effects. This regulation directly affects operational decisions concerning the construction of new power stations that use new technologies, the choice of SCADA systems and other electronic systems, and the types of fuel that they use. These decisions affect the mutual interdependence created between the infrastructures.

5. *Political and social factors.* These factors drive markets and choices, and constitute a basis for determining the necessity for laws and regulations, the level of providing services, the extent of protection, and the level of its implementation. The international, social, and political forces and interests also shape the infrastructure environment, since many of the infrastructures have become international. For example, the American electricity infrastructure is now merged with the Canadian electricity infrastructure. Other international infrastructures include communications, fuel, and gas. Political issues affecting processes include producing electricity from water in the northwestern Pacific Ocean, non-American ownership of American communications infrastructure, etc.
6. *Technology and information security*. Security failures in one infrastructure raise the level of risk and have a negative impact on security at other infrastructures. For example, when a municipal water system is powered by the local electricity grid, a successful attack against the electricity grid SCADA system, the water supply system is liable to suffer from interruptions. Security of the water system is a result of the level of security in the electricity supply system, and the same is true for a disruption or failure.

The sixth sphere of reference for assessing the mutual interdependence between infrastructures is coupling and responsive behavior. Three topics are distinguishable in this sphere.

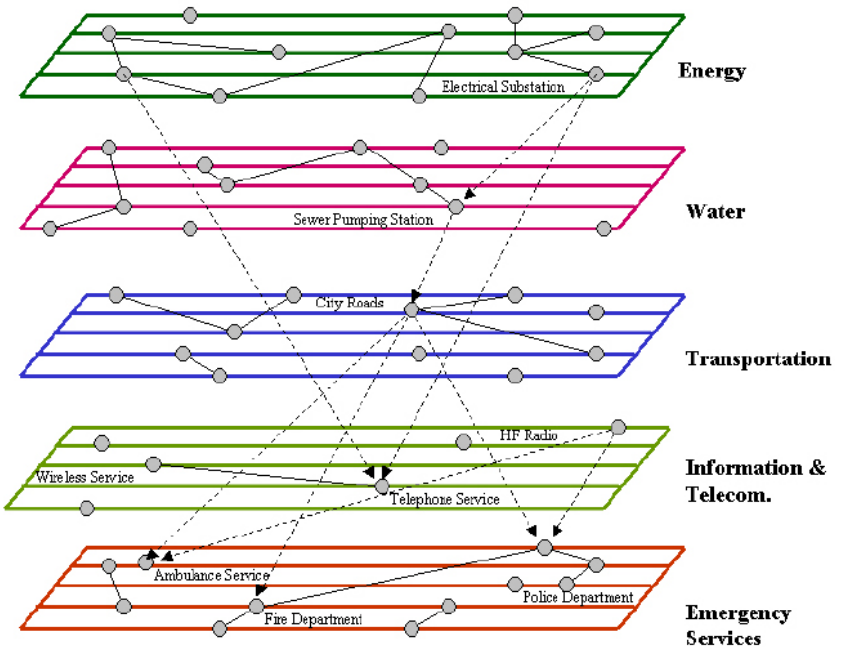
1. *Power: Tight or loose.* Tight coupling refers to infrastructures that are very dependent on each other. An interruption in one infrastructure is immediately linked to an interruption in the other infrastructure. One example of such a situation is a power station that runs on natural gas and the pipeline through which the natural gas flows. This coupling is especially close if there is no local gas reservoir, and if the power station cannot switch to using an alternative fuel source. In this situation, an interruption in the supply of natural gas will immediately cause an interruption in the production of electricity. Loose coupling exists when the infrastructure is relatively independent, and the state of one

infrastructure has almost no effect on the state of the other infrastructure. For instance, a coal-fueled power plant that usually has enough coal in storage for two to three months of operation, and the railway network used to transport coal to the plant. A temporary interruption in the coal supply does not immediately affect the functioning of the power station.

2. *Order: direct or indirect*. Direct coupling occurs when one infrastructure is directly connected to a second infrastructure. Indirect coupling is when the second infrastructure is connected to a third infrastructure; in this situation, the first infrastructure is connected to the third infrastructure through the second infrastructure, and the third infrastructure is therefore connected to the first infrastructure by indirect coupling. For example, an interruption in the supply of electricity will cause problems in the production of natural gas. That is direct coupling; further along the chain, enterprises that need natural gas for their operation will be affected, and that is indirect coupling between the supply of electricity and these enterprises.
3. *Complexity: linear or complex*. Linear mutual activity is part of a continuity of production or maintenance operations. At the same time, these operations, which are recognized and known, are likely to occur unexpectedly. Complex mutual activity is activity that is not part of the operational continuity, or is unplanned and unexpected, not in plain sight, and not immediately understood. For example, when a gas supply infrastructure is examined in isolation from other infrastructures, it can be regarded as if it were a linear system: gas flows from a given source to a gas stabilization plant, then through compression facilities and many gates, and eventually reaches the customer site. If the electricity production plant uses natural gas as a fuel source, and the electricity is used to operate the gas stabilization and compression plants, then the coupling between the gas and electricity infrastructures is in fact complex, not linear.

An example of a system of mutually interdependent infrastructures that affect each other can be seen in figure 2.

Figure 2: Mutual Interdependence between Municipal Infrastructures
(Pederson, Dudenhoeffer, Hartley & Permann, 2006)[12]



Source: Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory – INL: August 2006).

The diagram shows how infrastrucures in the municipal sector are linked to each other, are mutually interdependent, and affected by each other. As shown here, the municipal emergency services, for example, police, fire department, and ambulances, are dependent on the communications and transportation infrastructures, which are in turn directly dependent on the energy infrastructures. There is also dependence between the transportation infrastructure and the water infrastructure.

The following table displays the power of the dependence bewteen the various infrastructures at three levels: high, medium, and low. For example, the food industry is highly dependent on the electricity, water, and sewage purification infrastructures, and only slightly dependent on the natural gas infrastructures. Health services are highly dependent on

the supply of electricity and water, and the electricity infrastructure is highly dependent on the supply of natural gas.

Table 2: The Power of the Interdependence between Infrastructures
(Pederson et al., 2006)

Sector		Energy and Utilities					Services	
	Infrastructure	Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Hospitals and Health Care Services	Food Industry
	Electrical Power		H		H	M		
Energy and Utilities	Water Purification	H				M		
	Sewage Treatment	M	L			L		
	Natural gas	L				L		
	Oil Industry	H	L					
Services	Hospitals and Health Care Services	H	H	L	M	H		H
	Food Industry	H	H	H	L	M	L	

H – High M – Medium L – Low

Based on what has been presented thus far, it seems that a direct attack on critical infrastructure is liable to indirectly, and perhaps even directly, affect other infrastructures in the attacked country, and possibly in other countries as well, including the country of the attacker himself. These attacks are also liable to cause or facilitate war crimes.

For instance, an attack on a country's natural gas transportation infrastructure is liable to also affect energy production in additional countries connected to this infrastructure, but are not a party to the conflict. The attack on energy production can later cause damage to critical services and infrastructures in the energy sector and other sectors, including fatalities, disruptions at hospitals and especially in emergency rooms, damage to the operation of traffic lights at intersections, and interruptions of activity at critical enterprises.

An attack on a system used to manage computer infrastructure of a banking system is liable to disrupt processes and money transfers, thereby

causing direct damage to international companies. These are likely to include companies from the attacker's country.

An attack on infrastructures that operate a large port – such as systems for loading cargoes on cargo ships or oil tankers – is liable to affect all global maritime traffic: the entry of ships into the port will be delayed, thereby disrupting the timetables of shipping lines throughout the world. Ports belonging to the attacker are also liable to suffer damage. This involves large-scale loss of income and economic damage.

An attack designed to disrupt the operations of traffic lights at key intersections in order to delay the movement of forces to the front is liable to cause delays and disruption in the movement of ambulances and emergency and rescue forces. An attack designed to disrupt railway operations is liable to have a negative impact on the movement of goods and food. In certain cases, it is even liable to cause derailment, thereby endangering human life.

In addition, conducting a cyber-war is likely to be greatly affected by the interdependency and links between the infrastructures. International ownership of an infrastructure will affect both the attacker and the defender. The defending parties are likely to take advantage of the fact that the infrastructure that they are protecting is owned by an international corporation that also controls infrastructures in the enemy country. They can convince the enemy not to attack, so that his infrastructures will not be damaged as a result of the attack. Attacking parties are likely to find such international ownership very useful; they can use it to collect information on the infrastructure that they are seeking to attack, and perhaps to implant hardware or software for use during a future attack.

The Effect of Interdependence between Infrastructures on American Cyber Activity

The infrastructures' elements and the mutual interdependence between them affect their adaptation and flexibility. The Complex Adaptive System model characterizes a system according to its ability to learn from past experience and adapt itself to future projections. Many factors contribute to a system's adaptability: availability, the number of alternatives to critical processes or products, continuity plans for emergencies, backup systems, training operational personnel, and the creativity of the human factor in disaster situations. Other factors liable to make infrastructure inflexible include restrictive regulation and legislation, social aspects, organizational

policy, and fixed network topologies.[13] A collection of flexible components has a better chance of responding well to disturbances and continuing to supply critical goods and services.

The American modus operandi involves a framework and cyber cover for every military scenario. The aim is to be able to neutralize the enemy's defense systems before warfare begins, while providing security for the American fighting forces' information and communications systems. In this way, in addition to attacking the enemy's command and control systems, critical elements will also be attacked, and the enemy's ability to operate battle systems will be damaged.[14]

The doctrine that was established by the U.S. requires attaining and maintaining accompanying cyber supremacy for every battle action, according to the enemy's capabilities. The American strategy advocates cyber control over the potential enemies' command, control, and logistics deployments in an attempt to decide the campaign before it begins, and in order to attack these deployments as necessary later in the campaign, should one erupt. According to the American concept, kinetic activities cannot exist without cyber activities; in other words, operations in which conventional capabilities are used (kinetic armaments) will always be accompanied by operational cyber-capabilities. On their own, kinetic battles are no longer sufficient to achieve objectives in the best and most effective way, and accompanying cyber action is therefore necessary. In addition, any offensive action in cyberspace will be accompanied by preliminary collection activity – also in cyberspace.

In order to implement this strategy, the U.S. Armed Forces have established a cyberspace operational deployment with defensive and offensive capabilities, based on cyber command capabilities (based on the superior capabilities of the National Security Agency). In addition to securing the cyberspace in which the military systems and technological support for the kinetic units operate, the tasks include defeating any potential enemy and maintaining American supremacy in cyberspace, while attacking the enemy deployment in this domain. Defensive capability plays a decisive role in a conflict and in victory in the asymmetric cyber environment, such as that experienced by the United State. For this reason, there is an acute need to create balance between attack and winning capabilities and deterrent capabilities and defense.

In October 2012, President Obama signed Presidential Policy Directive No. 20, classified top secret, which outlines the legal infrastructure and

procedures underlying U.S. cyber policy. The directive includes guidelines for implementing criteria for operations by all American government agencies in dealing with threats in cyberspace. The basic terms relevant to cyberspace are defined, such as offensive and defensive operations, defense of networks, hostile activity, influence operations, and information collection in cyberspace. The need to develop and use cyber tools is also emphasized as an integral part of national power and security.

As revealed by Edward Snowden,[15] in Presidential Policy Directive No. 20, President Obama instructed the force to assess, among other things, the effect of these actions on parties liable to suffer damage as a result of their actions. Any activity liable to harm human beings, cause significant damage to American interests or substantial property damage requires presidential approval.

It is clear from the wording of the directive that its authors were aware of the possibilities of collateral damage resulting from mutual dependence between infrastructures. In this framework, actions will comply with the laws of war, and actions liable to have cyber effects within the U.S. require presidential approval. An effort should be made to locate every party liable to be affected by the action – both within the U.S. and among the enemy parties; actions liable to have significant consequences (by implication, for both American and foreign infrastructures) require presidential approval in ordinary times (in an emergency, there is a different process). Cyber operations carried out in response to enemy operations should be minimal in order to avoid significant consequences; during the discussion about the action, the effect on American interests should be considered, including damage to communications networks and infrastructures. Possible responses to and consequences of cyber actions affecting American interests should be mapped and appropriate preparation should be made in advance of the action.

On May 27, 2013, it was announced that the U.S. Joint Chiefs of Staff intended to give the commanders of the Armed Forces authority enabling them to use offensive cyber weapons in response to cyber threats, without requiring approval from the National Security Council. The procedures were agreed as early as 2010, but their approval was delayed due to a legal dispute about the operative authority and the force of the response to cyber-attacks. Only after prolonged staff work was agreement on this issue reached.[16]

The superior American technological capabilities rest, among other things, in the fact that most systems used in cyberspace are operated by American-owned corporations, while the majority of the non-American companies have a rapport with the U.S. As a result, the U.S. is clearly dominant in all facets of cyberspace including attack capabilities, and can deter potential enemies through the threat of an attack on them.

A cyber warfare campaign raises new strategic and defense issues:

Commanders must have a good knowledge and understanding of the systems and the occasionally changing technologies. Familiarity with the technology makes it possible to understand the significance of cyber warfare events.

Cyber weapons are not very expensive, nor does training the attackers require large-scale investment. These costs enable terrorist groups and countries with limited means to take part in cyber-warfare.

The fighting takes place on critical infrastructures and information systems that in most cases are also used by the civilian population. When the infrastructures and information systems are the front, technicians become combat soldiers who are likely to play a decisive role.

In the event of an attack on an infrastructure, the links between the infrastructures and the involvement of the civilian market in management of information systems and infrastructures might cause a far-reaching chain reaction.

The absence of regulatory legislation and the absence of an international convention on cyber-warfare make it harder to determine what is permitted and what is forbidden in such a conflict. In particular, there is a lack of clarity about attacks on civilian infrastructures.

The information systems and defense realms have changed greatly in recent decades. The U.S. utilized cyber-capabilities in the 1991 Gulf War, and it is known that covert cyber activity by American intelligence agencies took place years earlier. It is absolutely clear that cyber warfare will be part of any future modern conflict, and can sometimes even have a dramatic effect that will decide the conflict.

In past wars, U.S. forces have been accused of excessive violence, sometimes without scruples about harming the innocent. Cyber warfare enables American forces to operate moderately and with restraint, while attempting to avoid harm to those not involved. Furthermore, American policymakers have created an image in which the features of American culture and democracy place strong inhibitions and constraints on the use

of cyber power in an attack. Nevertheless, until Snowden's revelation, the American administration emphasized primarily defense against cyber-attacks, and publicly accused China of conducting cyber-attacks against it. The information revealed indicated that at the same time that the U.S. was accusing China, it had itself conducted offensive cyber operations against the Chinese government. In view of this exposé, China publicly revealed what it called the American "double standard."[17]

This was not the only allegation of American hypocrisy; duplicity is an important element of the "soft power" strategy used by the U.S. in order to persuade other countries around the world to accept the legitimacy of its deeds, even when they do not coincide with official declared policy.[18]

The direct interdependence between infrastructures is likely to mean that an attack on a military information infrastructure will cause a chain reaction that will affect civilian infrastructures. Attacking a country's critical infrastructure is liable to affect infrastructures and production capacities in other countries connected to the attacked infrastructure, and which are not a part of the conflict of which the attack was part. For this reason, such an attack is liable to result in war crimes, and even to damage American interests. It appears that an attack on purely military targets, such as radar and anti-aircraft systems, or core non-conventional weapons production and distribution systems, will be easier to carry out.

The interdependence between infrastructures requires those planning an attack on foreign infrastructure to carefully examine the connections between the target infrastructures and additional infrastructures in the other country as well as in the home country. Such an examination will allow for an easier attack through targeting connected infrastructure in which the attacker has discovered a weakness.

In our opinion, the U.S. will engage in information collection, and will also attack the enemy when the latter operate against American infrastructures. Attack weapons with a non-devastating effect may be used against the infrastructures in enemy countries, as well as target-focused attack weapons that can bypass systems not included as targets, such as Stuxnet. American policymakers will continue to promote an international law on activity in cyberspace, or at least international regulation in the framework such as the Tallinn Manual (sponsored by NATO),[19] or in reliance on the Budapest Convention.[20] They will also try to find moral solutions for conducting a cyber-campaign in events in which human lives are liable to be lost.

Notes

1 Federation of American Scientists, National Security Presidential Directives [NSPD] George W. Bush Administration, http://www.fas.org/irp/offdocs/nspd/index.html; Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, February 7, 2003.

2 *The National Strategy to Secure Cyberspace*, President Bush, Washington. February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

3 Lolita C. Baldor, "Pentagon Gets Cyberwar Guidelines," *Washington Times*, June 22, 2012, http://www.washingtontimes.com/news/2011/jun/22/military-gets-cyber-war-guidelines.

4 Patricia Zengerlensa, "Chief Warns Chinese Cyber-Attacks Could Shut U.S. Infrastructure," *Reuters,* November 21, 2014, http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121.

5 Eric Chabrow, "Obama to Congress: Enact Cybersecurity Laws," *GovInfosecurity,* January 21, 2015. http://www.govinfosecurity.com/obama-to-congress-enact-cybersecurity-laws-a-7816; Nicole Blake Johnson, "Lawmakers Welcome Cybersecurity Talks with Obama," *FedTech*, January 21, 2015, http://www.fedtechmagazine.com/article/2015/01/lawmakers-welcome-cybersecurity-talks-obama.

6 Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine* (2001): 11-25, www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

7 U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations" (April 2004), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf..

8 Jerry Gillette, Ronald Fisher, James Peerenboom and Ronald Whitfield, "Analyzing Water/Wastewater Infrastructure Interdependencies," Infrastructure Assurance Center – Argonne National Laboratory. Lemont, Illinois (April 2006), www.dis.anl.gov/pubs/42598.pdf.

9 The White House, "Critical Infrastructure Protection Presidential Decision Directive/NSC-63," May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

10 Rinaldi, Peerenboom, and Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies."

11 Federal Communications Commission, "Preserving the Free and Open Internet," December 21, 2010, https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.

12 Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory: August 2000).

13 Network Topologies- the network configuration and the defined connections between its components. In the current example the network has a defined configuration and cannot change.

14 Menashri, H. "Integrating Cyber-Warfare into Different Types of Warfare: a Case Study: the US," PhD dissertation (Ramat Gan: Bar Ilan University, 2014).

15 "Obama Tells Intelligence Chiefs to Draw Up Cyber-Target List – Full Document Text," *Guardian*, June 7, 2013, http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

16 Zachary Fryer-Biggs, "Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber-Attacks," *Defense News* (May 27, 2013), http://archive.defensenews.com/article/20130527/DEFREG02/305270014/Slowed-by-Debate-Uncertainty-New-Rules-Green-Light-Response-Cyber-Attacks.

17 Jonathan Kaiman, "China Reacts Furiously to US Cyber-Espionage Charges," *Guardian*, May 20, 2014, http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

18 Henry Farrell and Martha Finnemore, "The End of Hypocrisy - American Foreign Policy in the Age of Leaks," *Foreign Affairs*, November 2013, http://www.foreignaffairs.com/articles/140155/henry-farrell-and-martha-finnemore/the-end-of-hypocrisy.

19 Tallinn Manual Process, *NATO Cooperative Cyber Defense Centre of Excellence Tallinn*, Estonia. https://ccdcoe.org/tallinn-manual.html.

20 Convention on Cybercrime, *Council of Europe*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp.