Cyber Reliability, Resilience, and Safety of Physical Infrastructures

Cyber Reliability, Resilience, and Safety of Physical Infrastructures

S A Timashev[1,2,3]

[1]Sci.& Engng Center "Reliability and Safety of Large Systems and Machines", Ural Branch, Russian Academy of Sciences, Yekaterinburg 620016, Russia
[2]Ural Federal University, Yekaterinburg 620016, Russia
[3]Old Dominion University, Norfolk, VA, United States

E-mail: timashevs@gmail.com

Abstract. The paper considers the problem of constructing a full group of failure scenarios for physical infrastructures when subjected to cyber attacks (CAs). Physical infrastructures actually are systems of systems, or network of networks [1]. The main idea of the research rests on the assumption, that in order to damage any *physical* infrastructure by a *cyber attack*, it has to be able to produce a powerful enough physical impact on the most vulnerable part(s) of the infrastructure. Only civil engineering and industrial structures and installations connected to Internet and World Wide Web are considered. Hence, all infrastructures discussed below have to be elements of the Enterprise IoT or IoT, namely: electrical grids, oil, gas and product pipeline systems, water supply and disposal (waste) systems, rail networks, air traffic control and telecommunications (finance, commerce, business) networks, etc. The paper discusses how to construct a full group of scenarios of physical impacts on an infrastructure and how to calculate reliability, resilience and safety of infrastructures exposed to CAs. This paper should calm down the legitimate concerns of lay people about disclosing vulnerabilities of critical infrastructures, because it raises the awareness and offers infinitely much more to the *armor/shield* than to the *canon/spear*.

1. introduction

The history of cyber attacks on infrastructures started in early 1980s, when the Internet wasn't existing, and is in the process of shaping itself. In one of the very first official reports on small-scale cyber attack attempts against various U.S. electrical utilities [2], results are described of surveys of 15 cyber attacks and incidents over a period of three decades (sic, since 1982). None of them have caused significant damage or disruption [2]. At the same time a group of hackers installed a Trojan into the SCADA system which controlled a Siberian pipeline, which resulted in a powerful blast. The identity of the hackers was identified only 22 years later, when DoD USA Secretary under R. Reagan, Thomas Read published his book "*At the Abyss: An Insider's History of the Cold War*" from which we learned that the attack was organized by the CIA. This and all cases without reference described below come from the Internet source [3].

The next incident is dated by 1992 when a fired Chevron worker penetrated computers of the company in New York and San Jose and reprogrammed them for allowing leaks of poisonous gases from Chevron installations. This man-made hazard exposed thousands of workers to potential danger for 10 hours, before the system was restored for normal safe operation. Other accidents involving

cyber attacks were recorded in 1994 (the Salt River Project, where removal of files responsible for monitoring and logistics led to interruptions of serving electricity and water, and compromising personal and financial data), In 1997, the Worcester (Massachusetts, USA) airport was under attack that resulted in a six hour disruption of telephone communication at the dispatcher tower, fire fighters quarters and airport carriers' offices. In 1999 the Russian company Gasprom was attacked by hackers who, using help from an insider, used a Trojan to disrupt SCADA performance that controlled gas supply. The intrusion was curbed very early, without any serious consequences.

In 2000 a former employee of the Maroochy Water System (Australia) got two years in jail for hacking company's computers that controlled water supply that resulted in millions of liters of sewage entering an adjacent fresh water river and flooding of a hotel. In 2001 a US gas processing company was hacked by a supplier who did this to hide his logistics mistake. As a result gas supply was switched off in several European countries. In 2002 the PDVSA oil company in Venezuela was attacked during a strike. As result, its output went down from 3mln.b/day to 370 thousand b/day. In 2006 two engineers, experts in road traffic hacked out of protest the Los Angeles traffic lights, by making them stay red all the time that led to serious traffic jams. In 2008 a 14-year old student did the same with the tram (city cars) in Lodz, Poland. As a result, four trains went off track, 12 people were traumatized. In 2012 the offices of the world largest oil company, Saudi Aramco, was attacked grounding 30 thousand computers. Responsibility for this cyber attack was taken by a group that called itself "The Sword of Justice." In two weeks after that attack, the RamGas Company of Qatar was attacked by the same type of virus. As the result, the internal corporate web and its website were out of order for several days. Starting late in 2009, several U.S. natural gas pipeline operators came under a barrage of highly sophisticated cyber attacks related to industrial espionage, but they could be precursors to cyber attacks and/or physical attack [4]. In 2014 a German metallurgical facility was attacked by hackers who were able using social engineering to get access to an employee's computer through which they got access to the control system of a blast furnace. As the result the furnace could not be shut down, which resulted in great losses. In 2015 Ukraine's electrical grid was hacked and 600 thousand citizens were left without electricity.

The first in history massive cyber attack on a cyber system happened in 2007 in Estonia, when websites of its Parliament, ministries, banks, newspapers and other mass-media organizations, as well as the national system of processing telecommunication services and financial orders, went down. It was alleged that Russia is responsible for the incident.

The diagnosed malicious virus programs that were being used in the attacks were SQL Slammer that was tailored to attack data base servers (cases: US oil company, a major US automobile company). A hospital in Great Britain was attacked by virus Mytob. Virus Nimda was responsible for attacking a US food producing company. Air Canada, Mitsubishi Electric (sensitive inspection data about its two nuclear power plants were leaked as the result), Cook County, DOT, Illinois, USA were attacked by different viruses that were not made public.

The up to date first, largest and most elaborate cyber attack, that actually lead to significant physical damage of the infrastructure, was executed by a worm program called Stuxnet, on the Iranian centrifuge cascade for nuclear isotope separation in Natanz, Iran (Fig.1). The attack (which took place in 2008-2010) was preceded by extensive remote clandestine cyber diagnostics/monitoring of the target. Stuxnet gathered detailed information about the centrifuges and their control system, providing the basis for the development of a precisely-tailored worm attack tool. The general belief (not supported, as yet, by any fully trustable documents) is that Stuxnet was developed and inserted in the centrifuge cascade system by a concerted effort of the USA and Israel.

On the surface, Stuxnet was able to deceive the SCADA as to the true state of the centrifuge operating parameters at the same time that the centrifuges were forced to operate at speeds well over design values and, alleged, continuously changing the frequency of their spinning in time, thus causing the fatigue phenomenon in its mechanical parts and subsequent fast accumulation of high-cycle fatigue damage and rupture of its crucial details. Published damage estimates related to the centrifuges per se and the isotope separation process vary [5].

Figure 1. Cascade centrifuge facility in Natanz, Iran [3].

The motives in the above cases were industrial espionage, blackmail, reconnaissance for cyber or physical attack, and/or implanting code for later cyber attack [6]. Worldwide, there are no publicly known (as of 2018) military campaigns against the infrastructure of cyberspace, nor any military cyber attacks on physical infrastructures of any country. But a plethora of attacks were recorded by hackers of all hues and colors, and it is alleged that some of these attacks have been sponsored by (usually, not precisely identified) states.

Currently, already hundreds of cyber attacks are documented on critical infrastructures on all the inhabited continents (except, probably, Africa), but mostly, Europe, North America and Asia. Danger of a cyber attack on a critical infrastructure is real, and governments of all developed countries are well aware of this. After 03/11 2004 Madrid attack the EC developed *The European Programme for Critical Infrastructure Protection*. In May 2016 after the meeting of the G7, Energy ministers signed a joint Declaration in which they accented the need of implementing failure proof energy systems (including gas, electricity, and oil). Now G7 governments are creating centers for gathering data needed to improve safety of critical infrastructures. As a result, a complex strategy for solving this problem was developed, to be included into the national laws and ordnances of the G7 countries.

2. Some Definitions

For better understanding of the following, we start with a short description of some elements of infrastructure networks theory. From the point of topology, a network consists of nodes and links that connect the nodes in a specific fashion. The nodes represent the points of supply/origin and points of destination/ consumption. The links represent the routes of transmission/movement. The whole set of nodes and links comprises a network. A broad set of manmade, natural, and social systems can be represented and analyzed as this kind of transportation networks. Infrastructure networks are complex, irregular; and statistical in nature. Large networks can be classified as exponential networks (highly connected nodes are exponentially unlikely) and power-law networks (as they, typically, do not contain dominant nodes). In the first type of networks most of the nodes have approximately the same number of links. These kinds of networks are descriptively named as *uniform-random networks* URN (see Fig. 2).

In the second broad class of networks most nodes are connected to nodes that already have a considerable number of connections. This feature lead to describe them as scale-free networks (in the sense of number connections per node).The more descriptive term for this kind of networks is *hub-and-spoke random network* HASN (see Fig. 3).

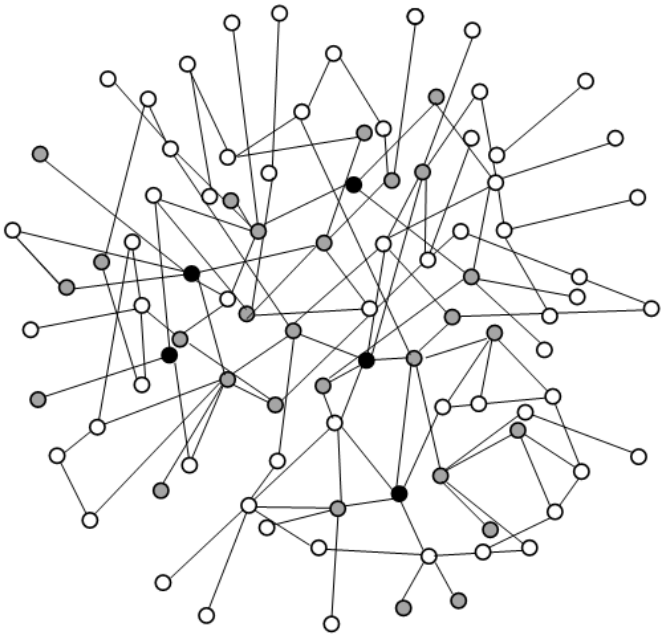

Figure 2. A typical uniform-random network infrastructure.

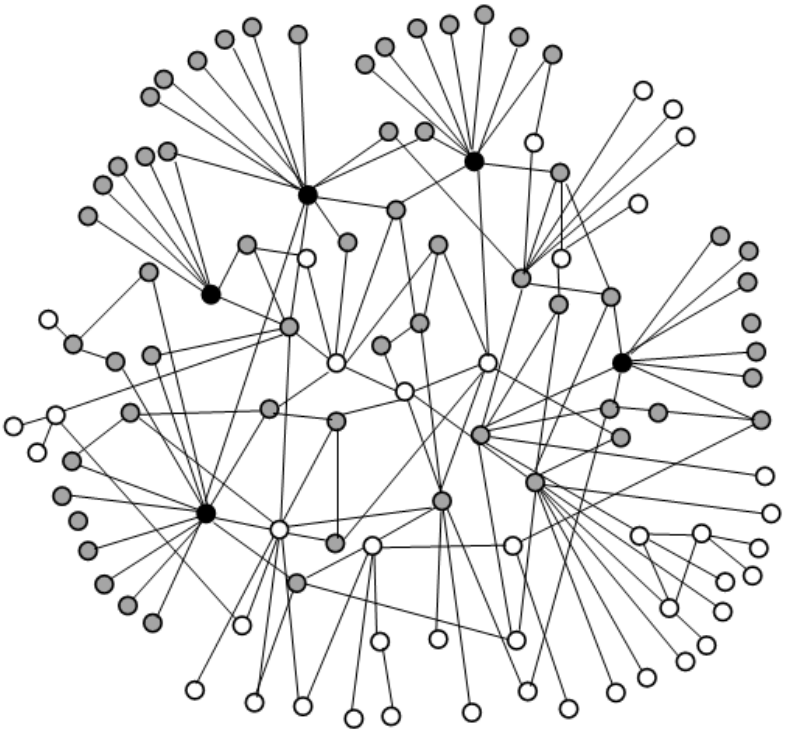

Figure 3. A scale-free infrastructure network.

A cyber attack that disables a randomly picked node from the URN (Fig.2) typically would disconnect only a few other nodes that are connected only to the disabled one. A random disablement

in the hub-and- spoke network would likely do even less damage, since so few nodes have any other node that connects only through them. However, in the worst case scenario for the scale- free network (when several nodes are disabled, see Fig.3), the damage will be greater than in a similar scenario for the exponential network.

3. Cyber Networks

The Internet, like practically our entire society, is critically dependent on electric supply. Both the Internet and World Wide Web (WWW) are scale-free networks. WWW is the *very first truly planetary scale digital infrastructure* (Fig.4).

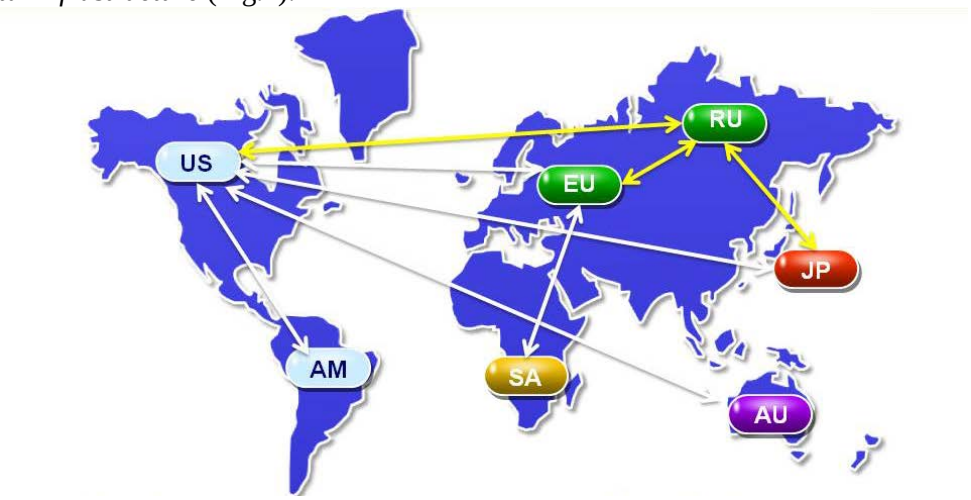

Figure 4. Russian computer network (RUNET) integrated into the global network [7].

Scale-free networks emerge usually through natural growth, as new nodes link preferentially to old nodes that are already highly linked. It is interesting that China didn't connect to WWW, it operates its own separate network, protected by a wall from WWW.

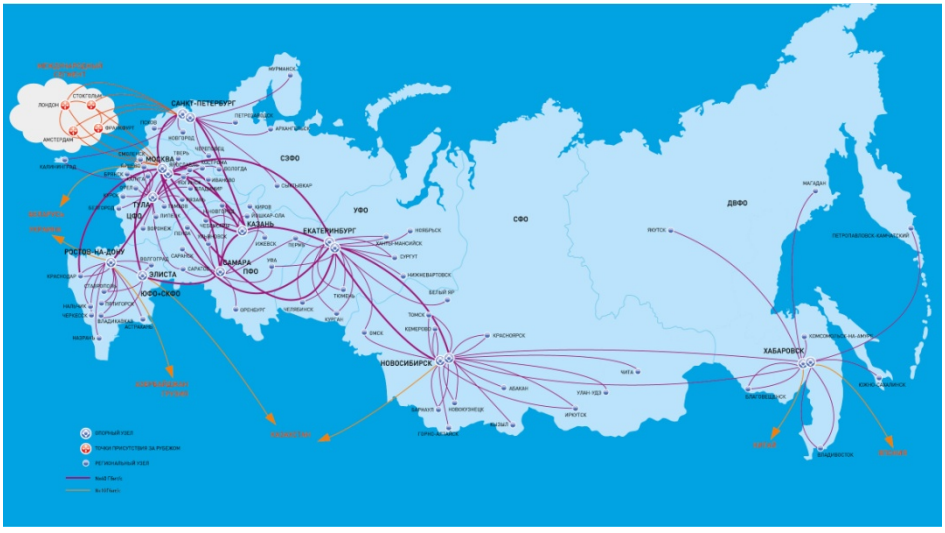

Figure 5. Backbone network of the Russian JSC Rostelecom [8].

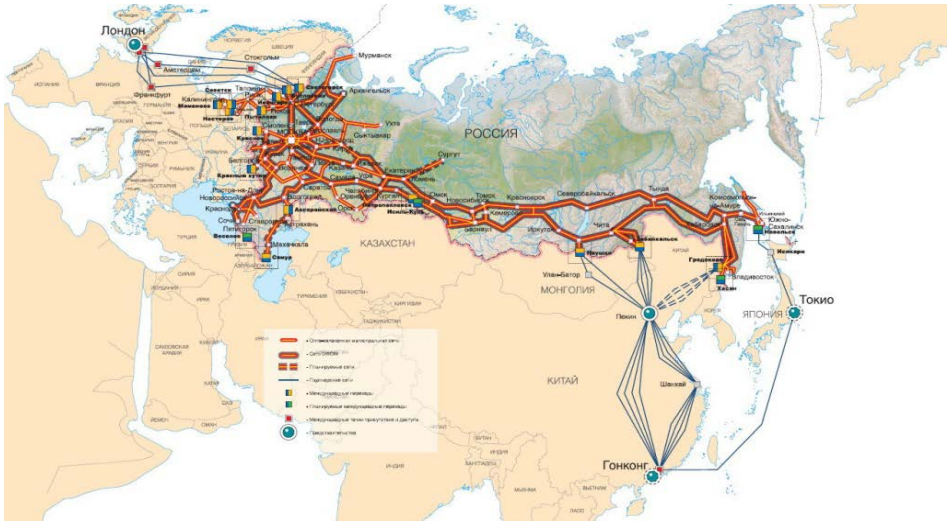

Figure 6. Backbone of a new Russian digital communication operator [9].

Currently, due to the observed weaponization of the Internet and WWW, they are subjected to particularly intense study of their capabilities, strengths and vulnerabilities [10]. Table 1 shows that the cyber content rests on a structure of physical elements that have physical properties and locations. It can be easily observed that cyberspace itself, like any other infrastructure, has its own geography and topology (the latter not identical with that of the network layers), and both affect its vulnerability and, hence, resilience.

Table 1. Schematic Description of Levels Involved in Cyberspace [1].

Level	Description	Examples
Cyber	Intellectual content	Data, commands, knowledge, ideas, mental models
Logical net	Services employing physical signals to carry logical messages	Telephones, broadcast radio and TV services, cable TV service, public Internet, private Internet protocol (IP)–based networks carried on common-carrier infrastructure, private-infrastructure IP- based networks, supervisory control and data acquisition networks
Hard net	Infrastructures formed from base elements that carry electrical or electromagnetic signals	Common-carrier telecommunications networks, tactical radio systems, dedicated wire line systems, community cable systems, cell phone systems
Base	Physical elements that underlie telecommunications services	Cable networks, optical fiber, coaxial cable, radio transmitters and receivers, radio transmission paths, communications satellites, Internet routers, modems

Internet nodes consist of computers (or devices that incorporate computers). Nodes are connected to an Internet service provider (ISP), which offers a connection to its hub or server bank (a cluster of high-speed computers) via some kilometers of telephone wire, coaxial cable, fiber optic cable, wireless cellular radio link, or satellite radio link. In their entirety, all these components comprise the current Internet architecture as a scale-free HAS network resembling that shown in Fig.2.

Scale-free networks are, for reasons described above, robust in the face of random or untargeted failures, which fall most heavily, according to laws of statistics, on the large numbers of nodes with only a few connections, and, hence, has scarcely any discernible effect on the overall network performance. Even more massive failures, due to widespread power outages, have been quite localized in their effects [11].

Successful attacks on many of the biggest hubs would have severe and pervasive effects. Hence, protection of major Internet hubs is a cornerstone of rational policy for cyberspace infrastructure defense, but keeping in mind that links that are logically and topologically separate may in fact be carried over the same physical communications infrastructure through multiplexing, via one fiber optic strand, or otherwise be vulnerable to the same damage agents. Thus, a single attack might take out thousands or tens of thousands of links, potentially cutting off multiple nodes from the network. The places where this can occur must be protected to assure cyberspace infrastructure integrity [1]. This is a particular concern for nodes located in geographically isolated sites (i.e., North Siberia, Far East of Russia), that are critical to national security. Loss of electricity does not ordinarily take down a major Internet hub – at least not at once, since most hubs have emergency backup power sources that can carry them for hours or even days.

Most modern infrastructure systems face profound transformation as a result of the fast moving technological and market innovations. Inevitably, such transformation involves greater reliance on cyber technology to improve the efficiency and effectiveness of infrastructure operation, and thus potentially further increases opportunities for cyber attack. This presents an ongoing challenge to regulators, developers, and operators.

Virtually all infrastructures of economic importance depend on information systems that are potentially the targets of cyber attacks. The latter can be classified by their intent as follows: 1) to provide information and garner specific knowledge needed for organizing a physical or cyber attack. The technique used here is similar to industrial espionage techniques; 2) to supplement a physical attack, in order to exacerbate the intended damage. These kind of attacks temporarily disable protective or corrective responses; 3) to damage or destroy critical physical nodes (for EG it would be electrical generators and large step-up and step-down transformers, for liquid pipelines--pumps, valves; for gas pipelines--compressors, valves, etc.).This kind of attack is the most difficult to organize, as it needs perfect timing, near-synchronous execution and extensive and precise knowledge of the intrinsic mechanical and material properties of the object being attacked.

With having in place operating personnel with high levels of diligence and compliance and security subsystems installed, the success of all types of cyber attacks on critical infrastructures can be severely limited and can be virtually nullified by rigorous reverse engineering. Reverse engineering is a way to design and operate existing infrastructures taking into full consideration system thinking of a malicious mind that is planning to execute a cyber attack on these objects.

To impose strategic-level and lasting physical damage to any major infrastructure system widely-dispersed over a territory (communication, electric, oil, gas, water, etc.), multiple quasi-simultaneous physical attacks on their most vulnerable nodes are required. Attacks on second-level nodes (transmission towers, separate single power generators, compressors, pumps, etc.), may be locally disruptive and costly to infrastructure providers and users, but yield only restricted damage and partial decrease of its productivity.

The design and manufacture of the damaged Iranian centrifuge cascade were inherently of marginal quality manufacture and inadequate materials for such highly stressed machines. It is doubtful whether Stuxnet or any other software worm would be successful against infrastructure systems with better design and more robust quality.

Government regulators and industry groups in general seek to provide balanced and integrated protection not only against cyber threats but the entire spectrum of natural as well as malicious threats. Infrastructure firms in general recognize their strong economic interest in protecting themselves and their investments, and for the most part are reasonably willing to comply with the state regulations [1].

4. Critical Infrastructure Vulnerabilities

Cyber Networks. The network levels that support and comprise cyberspace are run almost entirely remotely by computers without any direct human intervention. This opens widely the door to cyber exploitation and attack, to which they were more or less systematically subjected in the form of distributed denial of service (DDoS) attacks (the most common form of attack), as well as a variety of exploitation attempts. Motivations for the DDoS include *extortion*, *ransom*, *revenge*, *publicity for causes*, etc.

Reported intrusions [1, 3] have almost all been information-seeking, for criminal or obscure purposes. Remarkably, there have been no reports of coordinated cyber attacks attempting to exploit the damage and impede repair and recovery operations. But there is no guarantee that this will not change in the near future.

The Electrical Grid (EG) is the infrastructure of greatest concern in connection with cyber attack. The potential problems and solutions for other infrastructures broadly parallel those of the grid. The cyber security of the Russian electrical grid has been the subject of intense and broadly-based research for nearly two decades, allowing some fairly trustable conclusions. The topology of Russian EG resembles the HAS network of Fig.3, with some features of the UR network shown in Fig.2, with each generation source, transmission substation, or distribution substation as a node and each line connection of two nodes as a link. In this kind of transmission networks hubs connected directly to large numbers of nodes are rare and most nodes have more than one link, except for those in the fringes of the north-east parts of the Russian EG.

The fast and accelerating advent of the sixth tenor of technology will dramatically change the structure and layout of Russian electrical grids as it will become increasingly smart and hybrid, combining traditional energy generation (coal, oil, gas, atom) with renewable energy systems (hydro, sun, wind, ocean waves, bio-fuel, thermal, etc.), and some novel energy storage subsystems (high capacity batteries, flywheels, heat accumulators, etc.).

Currently the Russian state-owned unified EG is comprised of a relatively small number of large central station plants, usually located in the vicinity of their energy sources (Fig.6). Electricity is a bulk commodity that lacks specificity and is economically transmitted in the form of alternating current (AC) at high levels of energy and voltage, and most electrical use is AC at lower (220 v) voltages. Major production and transportation corridors are served by a few high-capacity HVAC lines along which distribution stations are located that feed local bulk users and local retail distribution networks, using the transformer as a passive device that allows economic tapping down high-voltage AC (HVAC) to lower voltage. The corridors follow the customers and, hence, are determined by economic geography (mostly, along the TransSiberian railroad).

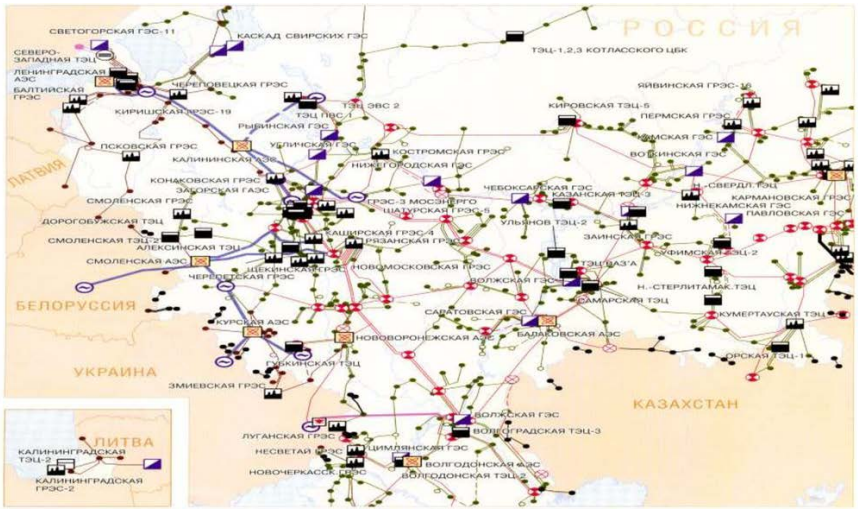

Figure 7. Unified national electric grid of the European part of Russia [12].

When the flow in an electricity network is near the limits of its capacity, the failure of one link could throw more load on remaining links than they can carry without overheating. This would lead to a cascade failure, due to overheating of links, one by one, or automatic /manual shutting them down to prevent damage.

On an AC network, the current must alternate precisely at the same frequency everywhere in synchronous operation. Any failure of this frequency synchronization would produce unbalanced forces that could literally tear equipment apart. If local overloading drags the frequency of a generator down, then it and the area it serves must immediately be disconnected from the grid [1]. Synchronization failures also can cascade, as generation or transmission equipment drops offline to avoid catastrophic failures. Within each of the regional grids the frequency must be the same at any given instant; misalignment of frequency between regions can be tolerated only if they are connected by DC interconnections, which serve as trip for a major blackout. This scenario, on a wide scale, can cut the grid up into isolated islands, many or all of which might fail under local load imbalances [1].

The loading on the grid varies from moment to moment. Users can randomly add loads by throwing a switch; generators and transmission equipment can go offline for a variety of reasons. Grid operators have a limited load-shedding capacity (temporarily cutting off customers who have bought “interruptible power” at reduced rates). In an emergency, a block of customers in a particular area may be blacked out to shed loads, but many systems are not set up to allow it to be done quickly, and utilities are reluctant to do this except as a last resort [1].

Could such a failure cascade engulf large regions of Russia and adjacent countries --former parts of the Soviet Union like Belorussia or Kazakhstan-- that are connected to the Russian EG? This scenario is highly unlikely, due to the fact that HVDC intertie lines isolate each region from frequency disturbances in other regions, and because disturbance from a major fault in the grid weakens as it disperses.

Because every part of the grid influences every other part, it has been difficult to construct a deregulation regime that would allow the truly independent operation necessary for fully effective competition. The same limitations that permit participants to impose costs on others without inherent limits (other than those interposed by the remaining regulators) equally allow serious technical problems to develop and spread without any individual participating firm or organization having a clear interest in taking corrective action.

The physics of electricity make it impossible for a fully disunited, every-entity-for-itself EG operating regime. If the system is to operate stably and safely, there must be some consistent set of operating rules that everyone is constrained to obey. This realization has been somewhat slow in emerging, perhaps in part because authorities were thinking in terms of analogies with networks that were not as tightly coupled as the electricity grid and thus less in need of highly disciplined operation.

SCADA and system management networks. All modern EGs and other infrastructure networks with *distributed equipment* generally have as their components *supervisory control and data acquisition* (SCADA) networks. The earliest SCADA nets (in 1950s) were immune to any types of cyber attack because of their fully isolated from the outer world dedicated transmission channels. EG equipment generally has *separate* control and limiting systems (inherited, by the way, from the eighteenth century steam engines). According to this strategy a modern generator has several trips: over-speed, overvoltage, overpressure, etc. The SCADA controllers enable operator command and provide feedback control to reach and maintain the commanded state. The limiters limit damage from inadvertent or malicious improper operator commands as well as system failures; hence, if need be, they can *override* the controller inputs [1].

Digitalization of SCADA (using programmable logic controllers PLCs that generally communicate digitally to a central computerized control system) while bringing important advantages of economy and efficiency also introduced potential vulnerabilities to cyber exploitation and attack. The energy management system (EMS) (or its equivalent in other types of infrastructure systems), which is at a level above SCADA, optimizes overall economics and feeds directions to the SCADA to adjust system operation accordingly. As both EMS and SCADA have been digitized the distinction between

them has grown less clearly defined and they are often referred to as energy delivery control systems (EDCS). Standards for cyber security of EDCSs and their subsystems have been available since the mid-2000s. Nevertheless, examination and testing continue to reveal a series of common cyber vulnerabilities in many EDCSs [13].

Analysis of major outages and blackouts worldwide from the cyber security point of view revealed EG design defects and demonstrated how tightly coupled the grid is and what this implies for its operation and protection [14]. It also discovered a number of hardware and software failures, together with faulty operational procedures and operator errors on the local and regional levels.

The typical scenario of a blackout practically always includes a cascading effect. The trigger of such cascade of failures may vary. For instance, the immediate cause of the 2004 blackout in North America that involved 50 million people without electricity for a long time in winter was a series of instances in which high-voltage transmission lines contacted trees that had been allowed to grow too tall into the lines' rights of way. Autonomous safety systems sensed the resulting ground faults and automatically disconnected the lines to prevent more serious damage and fires. The prevention of the cascade was not achieved due to poor training of the operators and their excessive reliance on limited and fallible warning and diagnosis systems [1].

The future electric power grid, according to current research, will take the form of a cellular type smart grid with smart control, able to adapt to failures in real time with limited if any degradation [15], regulated by adaptive software rather than governmental agencies, and with provision to take advantage of distant power sources. This means that future EGs will depend even more on cyberspace. Hence, essential efforts are needed to improve the reliability and efficiency of power distribution without any increase of vulnerability to cyber exploitation and attack [16].

Cyber attacks against electrical grid targets can usually be expected only to exacerbate and/or impede response to physical defects or casualties, whether natural, accidental, or malicious in origin. For the most part, the potential of cyber attacks against *undamaged, robust* systems of modern design will remain limited to more or less temporary disruption of operation. Currently, the only known vulnerability (coined *Aurora vulnerability* AV) [17], [18], is the possibility to hack into the control system of an *electric generator or other rotating electrical equipment connected to the grid* and throw the equipment out of phase, causing severe physical damage to the equipment.

The practical difficulty of doing wide-scale damage to the whole EG is increased by the heterogeneity of the equipment and control software, produced by several different manufacturers at different times. To damage a substantial portion of such EG a set of highly coordinated attacks would be needed. It would be easier to attack only a small number of key highly- connected nodes [19] to produce a big damage that would take many days and even weeks to repair/replace, restart and reintegrate the EG, because the supply of replacement high-voltage step-up transformers (needed to raise electromotive force to the levels needed for long-distance transmission) is limited, as is the capacity for manufacturing additional ones quickly. No means to destroy transformers purely by cyber attack has yet been revealed, but it would be unwise to assume that it could not be done in the future.

Pipeline Networks. Two other Russian major energy-sector infrastructures, oil and natural gas – pipelines are also networked infrastructures, with about 71,000 km of oil pipelines and 179,000 km of natural gas transmission pipelines [21]. Water, waste and many non-hazardous and non-flammable fluids (CO_2, steam, coal, mineral and paper pulp, milk, etc.) are also transported by pipelines.

In a pipeline network, the driving force is provided by pressure which must be controlled, but not nearly so tightly as the electromotive force of EG network. The pumping/compressor stations of oil/gas pipelines and multiple valves that regulate input/ output as well as routing within the network are automatically and remotely controlled. The slow speed of the flow, rarely more than 5m/sec, permits using simpler than in EG, SCADA systems.

The registered low-level sabotage successful cyber attacks on pipeline SCADA systems (usually by individuals with economic or idiosyncratic motives), have the potential to inflict only temporary and local disruption, resulting in economic losses and nuisance to the pipeline operators and their customers [1].

Figure 8. The main operating and planned oil and gas pipelines of Russia [20].

Central fresh water distribution and waste collection urban systems have been the target of sporadic attacks, almost always by individuals impelled by economic or idiosyncratic motivations. Like other pipeline systems, current fresh water systems use remote monitoring and control, and experienced some cyber attacks [22], which raised concerns about their cyber security [23]. For the most part, the low energies involved in local water systems makes them unlikely targets for severely destructive cyber attack. Moreover, they are engineered so as to make it all but impossible for waste water to enter the fresh water stream through *misalignment of valves* accomplished through cyber attack. In general, the damage that could be done by cyber attack seems to be limited to unpleasant and costly nuisances, by the exception of systems equipped by electrical pumping stations where the AV could be serious, or gas compressor stations, where surge of compressors could be organized. Specifics of many water/waste systems are that they are very old and deteriorated (Fig.9) which makes them absolutely not attractive to cyber attacks.

Research into the theory and experience of cyber incidents has resulted in a number of guides for sound engineering and operating practice. As we have seen, sound engineering and operations can go a very long way to protect infrastructure.

Human Factor is playing a leading role in critical infrastructure reliability, resilience, safety and security. In order to achieve reliability and resilience of CI rigorous application of existing guides and accumulated best practices is needed. In practice though, compliance has been considerably less than universal and thorough (due to ordinary inertia, reluctance to change, to master new knowledge and skills, or take on additional responsibilities) [1].

The private/public owned infrastructure systems that run on a for-profit basis usually pursue objectives that diverge sharply in financial aspects from the public interest regarding security against cyber attack. Corporate management tends to seek near-term profits, while the public interest is in spending on safety, not stakeholder's shares. On the other hand, infrastructure firms have strong incentives to safeguard themselves against threats that are a part of everyday business and may actually affect financial results. Threats that tend to be deprecated in management thinking can be categorized as follows: 1) Threats that occur at long, unpredictable intervals; 2) Threats whose financial impact is outweighed by the costs of protecting against them, viewed on a NPV basis; 3) Unimaginable (to the top management) threats even if rationally predicted to exist, because has no direct experience of similar threats; 4) Threats for which shareholders and the public (and their peers)

are unlikely to hold managers personally accountable because they are held to be unforeseeable or unavoidable; 5) the black-swan type threats.

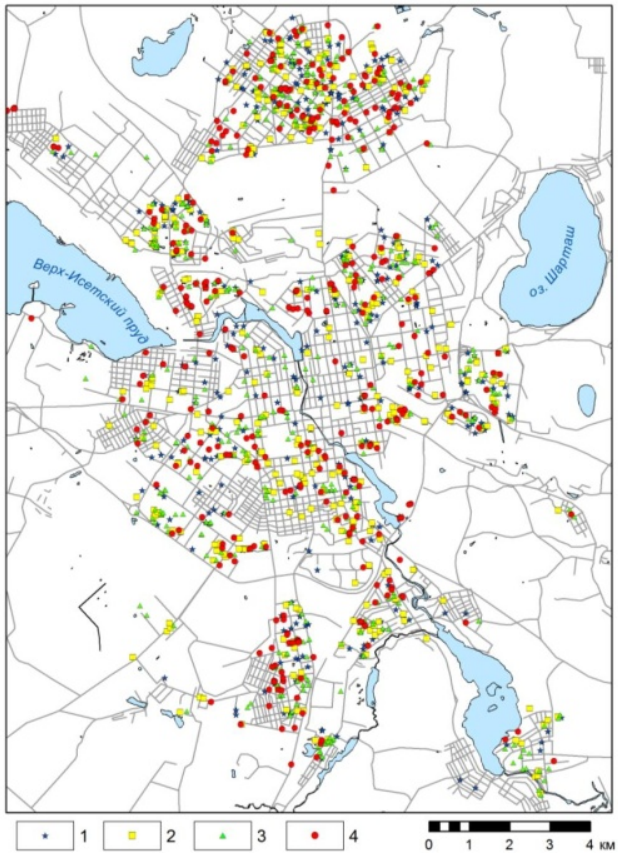

Figure 9. The City of Yekaterinburg: Scheme of emergency sections of urban water pipelines, (burst type of failure), for the period 2004-2007: 1 – 2004; 2 – 2005; 3 – 2006; 4 – 2007 [24].

In principle it is the responsibility of government to rectify imbalances between public and private needs by regulation backed by sanctions. In real life the advent of effective regulation almost always follows at least one catastrophe of a magnitude that draws widespread public interest. That's why progress on establishing effective regulations to avert cyber threats to infrastructure has been slow and halting. Moreover, the distinctions among threat sources—intrinsic, natural, criminal, or terrorist, often are not operationally meaningful: it can be difficult or impossible to discern the actual source of a threat in time to affect operations [1].

5. Problems of cyber reliability, resilience and safety of infrastructure systems

Generalizing all the above it is possible to formulate the hot spot problems of assessing and providing cyber reliability, resilience, and safety of modern infrastructure systems at all stages of their life time in the following form [25]-[27]. The cyber-problems are in a specific way inverse to ordinary reliability, resilience and safety problems, because the designer and operator of CI in order to meaningfully solve the above problems has to put himself in the shoes of the malicious adversary, whose goal is to damage or destroy the infrastructure being designed or in operation. Parsing the problem one would consider following inverse problems. Formulate new design schemes (mathematical operators of the CI under a CA) that take into account:

- existence of the SCADA subsystems (control, diagnostics, and maintenance) of the infrastructure proper;
- *full group of events-loadings*, that are generated by its own control subsystems, which were infested and/or influenced by viruses, and reflect the specifics of the cyber attack. For

instance, multiple simultaneous attacks on the most vulnerable components of CI, impossible at normal operation;

- new resilience and safety requirements to the personnel that operate critical infrastructures;
- imparting the CI with the «foolproof» quality against cyber attacks;
- formulate quantitative equations which allow assessing reliability, resilience and safety of different normal/usual operation, using classical and contemporary chapters of probability and uncertainty theories;
- include as obligatory quantitative assessments of reliability and safety of CI equipment that does not exist in ordinary design, but can take place during a cyber attack, i.e., non-stationary vibrations, resonance, gas turbine engines surge/pompage, water hammer, etc.;
- at the stage of design conduct assessment of vulnerability of the object as related to possible cyber attacks;
- explore vulnerability of CIs from the position of “wrong” control;
- conduct complex research of all possible new types of failures that are caused by cyber attacks.

6. Conclusion

1. The SCADA and EMS networks should be robust enough to continue providing accurate information and positive control even if subjected to coordinated cyber attack. Moreover, it is essential that operators be trained and adequately prepared to act resourcefully and decisively in response to casualties.

2. The foregoing examination of infrastructure protection issues has revealed that cyber attacks on physical infrastructures pose only a very limited strategic-level threat in and of themselves as long as right precautions are taken. This conclusion is broadly applicable to all well designed and manufactured major physical infrastructure systems.

3. Undependable software is one of the greatest vulnerabilities of infrastructure systems. The cost-driven trend to wide use of undependable and open-source software is exacerbating the risks. Software dependability will not achieve the necessary standards unless effective systems engineering is mandated for infrastructure systems.

4. While there is no clear limit to potential threats against infrastructures, there are limits to the resources that can be used for protection. Setting and keeping priorities for the allocation of financial and management resources are essential in order to provide effective protection.

5. The integrity of infrastructures affects everyone in our society, and the public will demand that its views be heeded. Hence, the public should be informed fully, clearly and accurately about all possible and happening cyber threats/incidents. This will ensure that the public will feel confidence in those who direct infrastructure protection efforts and will pay appropriate attention to their recommendations.

6. Policy direction for the various infrastructures should be tailored to their specific nature and needs.

7. Many important questions remain unsettled and more will arise as threats, technology, and economic conditions change. The Russian Federation policy and regulation institutions must have the authority, resources, and responsibility to sponsor and guide broadly conceived programs of research to serve their information needs. Knowledge can be expensive, but its absence can be much more so.

References

[1] Kramer F D and Starr S H and Wentz L K 2009 Cyber Power and National Security National Defense University (Center for Technology and National Security Policy) chapter 9

[2] Miller B and Rowe D 2012 A survey of SCADA and critical infrastructure incidents Proc. of the 1st Annual conference on Research in information technology pp 51-56

[3] Panda Security Rus November 30 2016 at 12:04 (https://habr.com/company/panda/blog/316500/)

[4] Lennon M 2013 Cyber Attacks Targeted Key Components of Natural Gas Pipeline Systems *Security Week*
[5] Kushner D 2013 The real story of Stuxnet *Spectrum IEEE* **50** 3 pp 48-53
[6] Gorman S 2009 Electricity Grid in US Penetrated By Spies *Wall Street Journal*
[7] Russian computer network (RUNET) integrated into the global network Available from: http://900igr.net/prezentacija/informatika/globalnaja-kompjuternaja-set-internet-99778/regionalnye-kompjuternye-seti-obedinennye-v-globalnuju-set-7.html [Accessed 28 Sept 2018]
[8] Backbone network of the Russian JSC Rostelecom Available from: https://www.expertsvyazi.ru/forum/printpage.php?forum=37&topic=4 [Accessed 28 Sept 2018]
[9] Backbone of a new Russian digital communication operator Available from: http://www.gudok.ru/newspaper/?ID=720435 [Accessed 28 Sept 2018]
[10] Krioukov D et al 2007 The Workshop on Internet Topology (WIT) Report *Computer Communication Review* **37** 1 pp 69–73
[11] 2003 Computer Science and Telecommunications Board *The Internet Under Crisis Conditions: Learning from September 11* (Washington, DC: National Academies Press)
[12] Unified national electric grid of the European part of Russia Available from: http://present5.com/vvedenie-v-elektroenergetiku-l-edinaya-energeticheskaya-sistema-rossii/ [Accessed 28 Sept 2018]
[13] 2011 Vulnerability Analysis of Energy Delivery Control Systems (Idaho Falls: Idaho National Laboratory)
[14] 2004 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* (Washington DC and Ottawa: U.S. Department of Energy and Natural Resources Canada).
[15] Farhangi H 2010 The path of the smart grid *Power and Energy Magazine IEEE* **8** 1 pp 18-28
[16] Yan Y and Qian Y and Sharif H and Tipper D 2013 A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges Communications Surveys & Tutorials *IEEE* **15** 1 pp 5-20
[17] Markey E J and Henry A W Staff of Representatives *Idem* pp. 4-5.
[18] Staged cyber attack reveals vulnerability in power grid Available from: http://www.cnn.com/2007/US/09/26/power.at.risk/ [Accessed 20 Aug 2014]
[19] 2012 Structure of the North American Electric Power Infrastructure *IEEE Systems Journal* **6** 4 pp 616-626
[20] The main operating and planned oil and gas pipelines of Russia Available from: http://fedoroff.net/publ/geography/geografiya/gazoprovody_rossii/48-1-0-576 [Accessed 28 Sep 2018]
[21] Herberg M E et al. 2010 Pipeline Politics in Asia: The Intersection of Demand, Energy Markets, and Supply Routes (National Bureau of Asian Research)
[22] Slay J and Miller M 2008 Lessons Learned From The Maroochy Water *Critical Infrastructure Protection* **253** (New York: Springer) pp 73-82
[23] Dakin R and Newman R and Groves D 2009 The Case for Cyber Security in the Water Sector *Journal of the American Water Works Association* pp 30-32
[24] The City of Yekaterinburg: Scheme of emergency sections of urban water pipelines Available from: http://shkolaput.ru/kaknsa/%D0%98%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5+%D0%B3%D0%B5%D0%BE%D0%B4%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9+%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D0%B8+%D0%B3%D0%B5%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9+%D1%81%D

1%80%D0%B5%D0%B4%D1%8B+%D0%B3+%D0%B5%D0%BA%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%BD%D0%B1%D1%83%D1%80%D0%B3%D0%B0a/main.html [Accessed 28 Sept 2018]

[25] Timashev S 2015 Infrastructure Resilience: Definition, Calculation, Application *Proc. of the WEEF Conference*

[26] Timashev S 2018 Resilient Urban Infrastructures – Basics of Smart Sustainable Cities. *IOP Conf. Ser.: Mater. Sci.* Eng **262**

[27] Timashev S A, AlekhinV N, Poluyan L V, Fontanals I and Gheorghe A 2018 Transforming Yekaterinburg into a Safe, Resilient-Smart and Sustainable City *IOP Conf. Ser.: Earth Environ. Sci.* **177**