Review scientific Paper/Pregledni naučni rad
Paper Submitted/Rad primljen: 25. 4. 2024.
Paper Accepted/Rad prihvaćen: 28. 6. 2024.
DOI: 10.5937/SJEM2402020M

UDC/UDK: 005.334:355.4
005.334: 504.4
005.334:[338.45:614.8

# Tehnološka i organizaciona pomeranja izazvana ratovima, prirodnim katastrofama i industrijskim akcidentima

**Branko Marković[1], Dejan Ilić[2], Ivana Ilić[3]***

[1]Bross Co. d.o.o., Bosnia and Herzegovina; e-mail: markovic_m_b@yahoo.com
[2]Faculty of Business Studies and Law, Belgrade, Serbia; e-mail: dejan.ilic@fpsp.edu.rs
3Faculty of Information Technology and Engineering, Belgrade, Serbia; e-mail: ivana.ilic@fiti.edu.rs

**Apstrakt:** Ovaj rad ima za cilj da pokaže uzročno posledične veze između bezbednosnih i operativnih rizika, ključnih bezbednosnih incidenata, i/ili promene bezbednosne paradigme usled dobre borbene prakse u ratu i načina na koji su se nakon ovoga pojavili novi ili evoluirali postojeći tehnički sistemi i organizaciona praksa. Kako evolucija tehničkih sistema zavisi od više faktora, cilj je da se u radu za navedene primere da kontekst evolucije i objasni kako je uticao na evoluciju tehničkih sistema i kasnije promenu organizacije. Takođe, za neke od navedenih sistema urađena je prognoza budućeg razvoja uzimajući u obzir poznata ograničenja, te je dato predviđanje ishoda za navedene tehnologije i organizacione modele u doglednoj budućnosti.

**Ključne reči:** operativni rizici, evolucija, tehnički sistemi, organizacioni modeli.

# Technological and organizational shifts caused by wars, natural disasters, and industrial accidents

**Abstract in English:** This paper aims to show cause-and-effect relationships between security and operational risks, key security incidents, and/or security paradigm shifts due to good warfighting practices and how new or evolved technical systems and organizational practices have subsequently emerged. As the evolution of technical systems depends on several factors, the aim is to give the context of the evolution and explain how it influenced the evolution of technical systems and the subsequent change of the organization. Also, for some of the mentioned systems, a forecast of future development was made taking into account the known limitations, and a prediction of the outcome for the mentioned technologies and organizational models in the foreseeable future was given.

**Keywords:** operational risks, evolution, technical systems, organizational models.

## 1. Introduction

Every major security incident is also a call to action, both political and regulatory, standardization, organizational and technical. The development of new technologies, that solve the problems of risk detection and its reduction or elimination, represents the basis on which public services, security agencies, the army, but also the economy, the banking, and the public sectors are later redefined. This is best seen when looking at how, after the attacks of September 11, 2001, in the USA, there was a redefinition of the public service and the role of the armed forces (Kennedy, 2017). Similarly, security incidents represent a source of innovative technical solutions designed to prevent the recurrence of a catastrophic event or other risks identified and confirmed through a security event. In this way, security incidents represent the starting point but also the context in which technical and technological solutions evolve and changes in organization and operations based on them.

## 2. The impact of technical, natural, and social disasters on technical and technological evolution

The mechanism responsible for the way and path of evolution of technical systems is not entirely clear, but the research conducted by the author Josef Taalbi clearly showed that it is possible to predict more than 30% of innovation patterns and ways of system evolution within the national economy (Josef Taalbi, 2020). As it is clear from the historical analysis of crises and critical events that after a critical event, a suitable solution is always sought to avoid its recurrence or reduce the risk, critical security events will almost always give rise to new technical and/or organizational solutions. In some industries such as aerospace, this has even been established as a regulatory requirement. It is also clear that wars, as the greatest social catastrophes, define new security threats and the ways and methods of responding to them. If we look at the war as a hierarchical network of events, it is clear that the war will influence the creation of a network of innovations that can be predicted based on the basic war processes, and especially based on combat and logistical requirements. The results of the author's analysis clearly show that there is a consistency in the fact that innovations appear in a synergistic form in such a way that technological systems that are shaped according to technological requirements and specifications are not always balanced, i.e. that successful and widely accepted solutions exceed the technical specifications that are given to them.

On the other hand, the research of the authors Kastelle, Potts, and Dodgson allows us to predict the way the technical system will evolve by observing the sets of rules that were valid at the time of the evolution of the technical system. Namely, viewing innovation systems as sets of macro rules within a micro-meso-macro system of rules has implications for how we attempt to view and manage technical and social innovation. In this sense, innovative systems must be viewed as populations (Tim Kastelle, 2009). Accordingly, their analysis should not only describe whatever rules currently dominate in any observed system into which evolution occurs but also consider the diversity within the associated rules.

This allows us to assess the dynamics of the system by measuring relative changes in the population of rules. It is very important to study Innovation Systems at all three levels of analysis - micro, meso, and macro. Most of the current research emphasizes only the macro aspect of innovation systems - the description of which rules are currently present in certain systems.

The disadvantage of this approach, which is reflected in the observation of only the present rules is that this set of rules does not say anything about the possible ways of system evolution for that set of rules that is either unlikely or considered impossible in specific conditions or goes beyond the limits of the system. This is precisely where the potential for system evolution and innovative solutions lies, which do not appear in the normal conditions of operation and existence of super systems. Critical events most often break these established and common rules of the super system and introduce a new set of rules that then determine the possible directions of development and evolution of both technical systems and, consequently, organizational and operational solutions based on these newly introduced (evolutionary) rules. We can systematize the possible ways of system evolution by analogy with the living world and the evolution of the living world in the way shown in the figure below.

## 3. Observed security risks and critical events, their wider technological context, and the evolution of technological systems and organizational models

The security risks that will be dealt with in this work are already known because they have already manifested themselves through a series of accidents, and natural or social disasters and have shown how much destructive potential they have. Although this potential is usually greatest at the first appearance of such risks, i.e. at the stage when they are not yet fully known and clarified, it can be transferred in a similar form to potential events in the future.

### 3.1. Terrorist attack on the USA on 9/11

The terrorist attack on September 9, 2001, showed numerous weaknesses of security agencies and services but also showed security failures at the level of civil organizations, as well as how these failures could be exploited by malicious attackers. As the biggest terrorist act since World War II, this attack was analyzed in detail and numerous weak spots and new attack vectors were detected. From this analysis came a series of requirements for improving security, as well as the systems used. Also, as a consequence of the observed attacks, several new technologies were developed that were supposed to significantly reduce the risks of such an attack being repeated.

In this sense, as a consequence of the terrorist attack, the following occurred:

- Widespread application of video surveillance technology and significant improvement in the application of this technology, which soon moved from CCTV systems to digital video cameras and DVRs, followed by the development of specialized software for reviewing large amounts of video content and identifying persons and vehicles, as well as the development of biometric systems for tracking individuals believed to be a security risk (Jessica Katzenstein, 2023). On the other hand, the mass application of surveillance over all public spaces, institutions, traffic, and even companies opened a debate regarding the relationship between trust (in the security system) and surveillance (Björklund, 2021), where different forms of surveillance were considered necessary and acceptable to forms of digital dictatorship (Liav Orgad, 2020).

- Development of technologies for monitoring and analyzing Internet communications and their mass application to monitor and prevent terrorist activities on the Internet. The demands for the development of these technologies have caused the development of software for the analysis of big data and tools for monitoring online activities (Dawinder S. Sidhu, 2007).
- Revision of security policies for all services and companies that were involved or the subject of a terrorist attack, which led to an agreement on the exchange of security information between government agencies, international agencies, and companies in sectors where the risks of terrorist attacks are expressed. This was pioneered by airlines that introduced mandatory locking of the cockpit before take-off to avoid similar attack scenarios and the use of civilian aircraft as a means of attacking critical infrastructure.
- Development of a whole range of solutions in construction and building management, as well as evacuation systems in commercial and residential buildings. These solutions include external evacuation systems, the mass introduction of internal video surveillance, and the BMS system (Rae W. Archibald, 2002).

### 3.2. Fukushima nuclear accident as a result of the earthquake and tsunami

The accident at the Fukushima 1 nuclear power plant caused by the consequences of the catastrophic earthquake in Japan in 2011 showed the safety weaknesses of nuclear power plants against major natural disasters.

In response to these security weaknesses, the IAEA developed the Nuclear Security Action Plan, which included the definition of a program to strengthen nuclear security at all nuclear facilities in the world. Initiatives such as the European Stress Test and the adoption of the Declaration on Nuclear Safety in Vienna defined the lessons learned in the field of nuclear safety as well as how to develop disaster response plans, and how to understand prevent or minimize the radiological consequences of nuclear accidents both regionally and internationally at the global level (IAEA, 2024), (IAEA, 2021).

### 3.3. Evergreen container ship stuck in the Suez Canal

Due to an unfortunate jamming, the stranded ship Evergreen in March 2021 created a total blockade of the passage through the Suez Canal. This maritime incident resulted in not only a temporary blockade of the passage through the Suez Canal and a consequent delay in the transport of goods but also demonstrated in a plastic way the vulnerabilities of the chains of creation and delivery of value and ultimately of the global economy. Incidents like this one and the one involving the Dali ship in April 2024, when the Baltimore Bridge collapsed and one of the largest ports in the USA was closed, showed that a global economy based on mass transport of goods and dispersed production is no longer possible, that is, it has reached its limits possibilities of its expansion. The crisis caused by the pandemic of the COVID-19 virus showed the same.

In this sense, as a result of the incident, a large number of manufacturers, as well as retail chains, began to re-apply intermediate inventory methods and return the production of critical goods closer to the target market, thus Toyota's paradigm of JIT (eng. Just in Time), which for years was dominant in managed production and on which international trade was largely based, ceased to be the dominant economic-production paradigm. Additional security measures are newly developed software tools and international agreements and standards that provide better insight into supply chains, which on the other hand directly affect target markets not only by increasing the level of security of supply and excluding the part of trade that was usually associated with speculative actions, but which is more important for this market by removing part of the uncertainty that was an integral part of business on the stock market in all countries.

Namely, the increased visibility changed the habits of investors and therefore caused shifts in economic branches, especially those that were largely dependent on imported goods. Solutions that have translated supply chains into agile, with real-time control mechanisms are a direct consequence of these accidents and natural disasters (Özden Özkanlisoy, 2021). Also, the analysis of the incident led to a conclusion that applies to all types of traffic and sports. Namely, there is a noticeable trend in the growth of transport systems, whether it is vehicles, trucks, ships, or air transport, while at the same time, the supporting transport infrastructure is changing and growing too quickly, and as a result, the risk of similar accidents occurring again in the future is increasing. If this happens at critical points of traffic routes, this can cause a significant delay in transport, but also a complete interruption of supply chains (Rob A. Zuidwijk, 2021), which makes the economy based on the JIT paradigm significantly threatened and practically unsustainable in the future.

## 3.4. The war in Ukraine

The special strategic conditions created by the Cold War, characterized by the mass application of nuclear systems, have led to states conducting a ritual style of war, in which the demonstration of strength, instead of the physical application of violence (or the possibility of applying it in a real war conflict), becomes increasingly important. Within this environment, states have pushed the process of technological innovation in defense to extremes to demonstrate their military superiority (Warren Chin, 2019).

This massive peacetime investment in defense technology had a huge impact on the character of war (and other forms of conflict), leading to new strategic forms of it. On the other hand, the spread of military technology also affected the economy and society, which led to a form of internal transition of power within individual states. As the first open military conflict of the confronted parties in the Cold War, the Ukrainian war opened up the possibility of trying out new technological solutions in a real war environment, but also to rapidly evolving responses to them. It was this circumstance that influenced the war to become not only an engine of innovation, but also an opportunity to test some development ideas in reality. Running these ideas, especially if they prove to be successful, represents the initial step in the development path of new systems and consequently security procedures, organizational forms, and management models.

### *3.4.1. The emergence of mass use of drones*

The course of the war in Ukraine has shown unequivocally that there has been an operational and technological shift from expensive and complex unmanned aerial vehicles with integrated complex combat systems to the production and then operational use of small, low-cost consumer drones that can be mass-produced (Paul Schwartz, 2024). The reasons that led to this shift are numerous: from the impossibility of integrating complex systems into combat operations in wartime conditions, over the price which plays a big role not only in terms of procurement but before the estimated life span and losses on the battlefield, to ease of use, production and procurement of consumable simple drones.

### *3.4.2. Application of hypersonic weapons and tools*

Analyzing the war in Ukraine confirmed earlier allegations that hypersonic vehicles (missiles and drones) were developed, that is, the war clearly showed a sudden jump in the use of these types of weapons. What is an important change, not only in terms of changes on the battlefield but also changes to the ratio of forces and potential of the world's largest armies, is the possibility/risk of rapid neutralization of the key carriers of military potential and strength. Namely, there was an articulated and formulated threat that the use of such weapons could easily neutralize and sink aircraft carriers in a real war conflict, which is the crucial military potential of the USA and several other NATO countries (Centre for Joint Warfare Studies, 2022). This development significantly changes the balance of power and represents the first clearly expressed threat to US military dominance since World War II (Congressional Research Service, 2024). As the global world order and economic globalization are based on free sea trade, which is mainly ensured by the US naval forces, this is the first serious risk to existing economic relations and established flows of technological, economic, and economic cooperation in the world.

To examine this risk and take all the necessary steps to prevent such a scenario, the following measures are being implemented today:

- Development of systems for defense against hypersonic missiles. As a countermeasure, the military-industrial complex of the USA is now working hard on the development of laser weapons (Christopher McFadden, 2024; Emma Helfrich, 2020).

- Massive influence on the media reduces the perception of the danger of this type of threat among citizens and creates the belief that it is much smaller than it is. This trend is also clearly visible within academic institutions and technological think (Dmitry Stefanovich, 2021).
- Development of systems that could assume the role of primary pillars of military power. Military analyst Kyle Mizokami believes that the time of dominance of large warships is over and that in the future they will be replaced by smaller ships built on a larger scale and/or completely new platforms that will have a similar role (Kyle Mizokami, 2024; Brandon J. Weichert, 2024), because drones massively take over certain roles that were played by planes and ships, can be significantly smaller and therefore faster and have a higher probability of survival, but also lower costs of construction and exploitation. Parallel to this, changes are visible on the organizational level (U.S. Naval Institute Staff, 2024).

On the other hand, there is also a visible desire to use as many advantages as possible of this type of weapon and to adapt them for use in as many different scenarios as possible, so Russia insists on the development of interoperability systems and the use of hypersonic missiles with as many combat platforms as possible

#### *3.4.3. The appearance of robots on the battlefield - the robot as a weapon system, the robot as a tool*

In the previous phase of the war, it was shown that the evacuation of wounded and injured fighters in real combat conditions (which includes the extraction of the wounded under fire) led to large additional losses, so in the developed phase of the war (April 2024), robots, i.e. UGV (Unmanaged ground vehicle), for these and similar realistic war scenarios, whether it's about logistics or extracting the wounded. There is ample evidence that the real application of this new technology has occurred (TASS, 2023; Alistair McDonald, 2024; CNN, 2017; Cameron Henderson, 2024).

The primary goal of this technology is not to replace humans in risky environments and combat actions but to redefine the composition, equipment, and way of using combat units. The development of this technology came through a series of iterations made by both warring parties. There is a visible shift from a remote-controlled casualty recovery vehicle that has limited combat range and deployment to an autonomous combat and logistics system that is based on merging known non-combat platforms with scenario-defined AI agents. Although the RAND Institute rated such systems as systems of limited applicability (because they are guided remotely and it is possible to interfere with the signal) (David Axe, 2024; Tarraf, 2020), now a significantly stronger resistance to interference is already noticeable, which is achieved by the simultaneous application of MESH, a network for transmission of control signals and built-in artificial intelligence agents for defined combat scenarios.

#### *3.4.4. Development of potential - nuclear-powered cruise missiles and use of nuclear weapons in space*

Although the SDI project (SDI-Strategic Defence Initiative) of the American president Ronald Reagan was forever abandoned as unnecessary after the fall of the USSR, today we see the significant development of armed systems that were announced at the time but never fully realized (mainly due to the high cost of development and lack of adequate argumentation to justify the necessary spending of money from the budget). However, after several months of war in Ukraine, Russia decided to enter into the development of certain weapons and tools as part of its military efforts, which seemed unnecessary, unjustified, too expensive, and finally impractical for use in a real war scenario.

Two weapons systems stand out in particular because they have unforeseeable implications: the application of nuclear propulsion for cruise missiles, because the application of this system could enable the launch of cruise missiles from domestic territory and hitting the target anywhere on earth (Timothy Wright, 2023), and the possibility of they are using nuclear warheads in space that could be weapons for the mass disabling and destruction of all satellites (Kari Bingen, 2024).

As today's armies and civil societies rely significantly on satellite communications and signal transmission, this would give the party that uses such weapons the opportunity to cancel any transmission of signals either over its territory or globally, which would make it significantly more difficult, and in some cases even completely impossible, to provide internet services and military satellite services. As these are concept-based systems, that have never been tested (at least there is no clear indication that experiments with these systems have been successful), in practice the level of security threat is not clear, but it is clear that the threat is global and has the potential to in a short period, the balance of power, whether military or economic, changes, which is especially important for those economies that are based on the provision of Internet services. On the other hand, the application of the 9M730 Burevestnik missile would certainly have significant environmental consequences because the engine emits radiation throughout the flight, even if the missile is not armed with a warhead (Leah Walker, 2020).

As there is currently no clear indication of the effectiveness and reality of such systems, we can only state based on previous examples that there probably exists and is developing a suitable technology and a solution based on it that would neutralize or at least reduce this threat.

#### *3.4.5. Use of sanctions as a weapon*

As is visible from the volume of the Russian economy, and especially its growth in the period 2022-2024, sanctions as a way of economic warfare do not give adequate results. How the sanctions introduced by the USA, the EU, and Canada are implemented in Japan do not give the expected results, and the primary reason for this lies in the fact that Russian companies have managed to create a network of intermediary legal entities in friendly and neutral countries, and through them practically circumvent the imposed sanctions. A mechanism that is particularly interesting in this regard is visible from the congressional hearing of the international expert Ryan Berg, where the mechanism of the "ghost tanker" was explained (Ryan Berg, 2023; Ryan C. Berg, 2023).

This term refers to tankers under different flags, which sail with their transponders turned off, so it is difficult or impossible to locate them, and which most often transfer their cargo on the open sea, from one ship to another, to bypass sanctions and transfer oil or other derivatives on seemingly legitimate ships and finally sold precisely in those countries that have established and implement sanctions. What is now visible as an attempt at innovation is the creation of clear mechanisms for the control of trade at sea and the total visibility of value chains. These initiatives also have their civilian application - the application of the blockchain mechanism to all transactions related to goods starting from the place of origin of the goods to the place of consumption, which could have significant implications on the food and energy markets (especially today when it is insisted that the energy used originates from renewable sources). It is this component - a set of rules related to civil application that will provide, it is already obvious, the necessary means to develop these technologies and use them more massively.

Finally, we can show the chain of events and responses to critical security events and risks that have manifested themselves in the current course of the war in Ukraine as follows by introducing feedback links into the chain of events.

### 3.5. The war in Gaza

The war in Gaza is another conflict that threatens to redefine the boundaries of the known world, both in terms of the development of military technologies and war activities and in terms of a changed security paradigm in countries where tensions between social, national, or interest groups are visible and expressed. Although this war, in terms of the way the conflict was conducted, can be considered a logical evolution of the "Arab Spring", another conflict in the region that in the Arab world resulted in a significant change of forces and finally the change of certain regimes. What started then as a mass application of the Internet and social networks as a platform for organizing demonstrations has evolved in such a way that the applied paradigm also received its logical extension in the direction of application to military, that is terrorist activities. But the most important direction of evolution was not the use of Internet services as a communication platform and a single command post, but the use of the Internet as a tool for the evolution of production capacities and the arming of combat units and terrorists.

#### *3.5.1. DIY weapons and using the Internet as a communication channel for a terrorist attack*

The surprise attack on the Israeli kibbutzim and the music festival was carried out simultaneously in several locations with weapons that could not be considered sophisticated, and according to subsequent reports from the field, were home-made. The application of a popular online training model known as

DIY (Do It Yourself) has allowed Hamas terrorists to produce a relatively large number of weapons and ammunition, and to train for actions that far exceed the usual level of operations for terrorist groups. This is exactly what the security services did not expect and what led to a serious security breach that was used for the terrorist attack that started the war. Later reports from the field indicated the use of DIY weapons and ammunition by Hamas and other Palestinian units (McKay, 2023; NDTv, 2023). This is not an entirely new logistics strategy (The Guardian, 2016). Although this is mainly about primitive weapon systems and tactics, it is clear that the innovative way of manufacturing, equipping, preparing, and carrying out military operations was such that surprise and a series of easy military victories were achieved, which caused the escalation of the conflict. In retrospect, it becomes clear that what some security experts pointed to as a possibility when numerous sites appeared on the Internet where instructions on how to manufacture weapons and ammunition could be found in the public domain (Ragnar Benson, 1992; Integrated Micro-Electronics, 2022), today it becomes a real security risk that must be taken care of.

The world has not had the opportunity to see security failures of this nature and dimensions since 2001. Western governments and societies are particularly concerned about the possibility of using DIY weapons and tools by rebel social groups, especially in the scenario of climate migration, so they are already working on controlling internet content. Although similar measures were foreseen and implemented even after the terrorist attack in 2001, it is clear that they did not represent an adequate and satisfactory solution, so finding new solutions for dispersing security threats is still being worked on, and we should expect the emergence of new generations of solutions that would combine the logic of supply chains and the search for a related entity, but how far we are from real solutions in this area remains to be seen.

## 4. Possible new solutions and organizational models, trends, and possible outcomes for the observed technologies

As can be seen from the previous examples, certain technical and organizational solutions always have their sources in security risks (when they are articulated and measurable) or in security incidents (when previous security risks were not noticeable or validly considered in system development). Each security incident acts as the initial point of technological and organizational innovation, but also as the context of the same, and thus represents a set of rules in which evolution takes place. In this way, security incidents and the dynamics of the development of security threats act as a decisive factor in determining the direction of technological evolution and thus the outcome of evolution, that is, the appearance and characteristics of a new technical solution or organization established around it.

The terrorist attacks of September 9, 2001, the accident in Fukushima, and the war in Ukraine and Gaza represent significant security incidents that have conditioned or still condition the development of new solutions that strive to establish a security framework that guarantees the basic principles of the safety of citizens and property in situations that are similar to those who were present at the time of these events. As the war in Ukraine and Gaza is still going on, it is possible to expect some more significant security shifts, but the main trends in the evolution of technical systems have already been established by the mass use of drones, hypersonic weapons, and cheap, disposable weapons.

Also, it is clear that the DIY paradigm significantly changes the security environment and that in the future new efforts can be expected to use economic and industrial capacities as weapons. In this sense, some organizational measures have already been developed against turning the energy supply into a weapon - which led to the creation of energy security paradigms. Individual technical systems will have to converge and integrate under the influence of security triggers embodied in key events. Rapid advances and convergence in areas such as applied robotics, IT, and artificial intelligence will continue to have a revolutionary impact on the battlefield of the future (Daniel C. Billing, 2021). The disruption associated with these technologies will be most acutely experienced by the human warfighter at the tactical level, with increasing cognitive demands associated with mature wartime workloads that will grow as the demand for and use of new capabilities grows. In the long run, this is not a sustainable model, and there must be a change in the way units are organized and the way external operations are conducted.

## 5. Conclusion

From all of the above, it can be seen that there are cause-and-effect relationships between security and operational risks, key security incidents, and/or changes in the security paradigm due to good combat practice in the war and how new technical systems and organizational practices emerged after this or evolved surrounded by technological solutions, such that they have a complex and adaptive character. As the evolution of technical systems depends on several factors, their influence is not always clearly measurable or even noticeable, but the following chain is visible from the examples mentioned:

1) Emergence of new technology => 2) Security analysis => 3) Technical specification => 4) New technological solution => 5) New organizational form => 6) New way of conducting operations

This chain is inextricably linked with the chain of technological innovations, but in such a way that these two chains are multiply connected and mutually influence each other in many places and with more than one feedback loop. This is also the reason why it is not possible to apply simplified models, such as the Ishikawa diagram, but for a more correct description of the influence of individual factors of evolution, it is more adequate to apply feedback models that are applied for complex adaptive systems, such as the Vansim model. Key security incidents always precede the development of new technologies and organizational solutions that could not be perceived or were not given an agreed priority because these events were considered unlikely. In this sense, a security incident is not only a confirmation of the reality of the threat but also an environment that will further determine the way and direction of the system's evolution. In principle, the system will evolve until it reaches a balanced relationship between the threat, that is, the perception of the threat, and the resources necessary to satisfy the development requirements that have been reached by analyzing a critical event (incident or accident).

## Literature

1. Alistair MacDonald. (2024, 03 24). *Robots Are Entering the Ukraine Battlefield*. Retrieved from https://www.wsj.com/world/europe/robots-are-entering-the-ukraine-battlefield-fab195d2
2. Björklund, F. (2021). Trust and surveillance: An odd couple or a perfect pair? In L. A. Viola, & Paweł Laidler (ed.), *Trust and Transparency in an Age of Surveillance* (pp. 183-200). London: Routledge Studies in Surveillance. doi:https://doi.org/10.4324/9781003120827-14
3. Brandon J. Weichert. (2024, 03 06). *Aircraft Carriers are Obsolete: Let the Age of the Submarine Begin*. Retrieved from https://nationalinterest.org/blog/buzz/aircraft-carriers-are-obsolete-let-age-submarine-begin-209886
4. Cameron Henderson. (2024, 04 03). *Watch: Russia uses stretcher robot to save wounded soldiers*. Retrieved from https://www.telegraph.co.uk/world-news/2024/04/03/russia-stretcher-robot-save-wounded-soldiers-ukraine/#:~:text=Russian%20soldiers%20have%20begun%20using,under%20Ukrainian%20fire%20near%20Avdiivka.
5. Centre for Joint Warfare Studies. (2022). *RUSSIAN HYPERSONIC WEAPONS.* Centre for Joint Warfare Studies. Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cenjows.in/wp-content/uploads/2022/08/Russian-Hypersonic-Weapons.pdf&ved=2ahUKEwjjgMD607eFAxXQg_0HHUh4BJwQFnoECBQQAQ&usg=AOvVaw0lv7vEarANKYRC1BJuEAJv
6. Christopher McFadden. (2024, 03 22). *Scientists find ideal laser power to kill hypersonic missiles — China*. Retrieved from https://interestingengineering.com/innovation/ideal-laser-power-to-kill-hypersonic-missiles
7. CNN. (2017, 04 25). *This Russian robot shoots guns*. Retrieved from https://www.youtube.com/watch?v=HTPIED6jUdU
8. Congressional Research Service. (2024). *Hypersonic Weapons: Background and Issues for Congress.* Congressional Research Service. Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://sgp.fas.org/crs/weapons/R45811.pdf&ved=2ahUKEwjjgMD607eFAxXQg_0HHUh4BJwQFnoECA8QAQ&usg=AOvVaw0VctfcRSzuaqKxgY-QCnco
9. Daniel C. Billing, G. R. (2021). The implications of emerging technology on military human performance research priorities. *Journal of Science and Medicine in Sport, 24*(10), pp. 947-953. doi:https://doi.org/10.1016/j.jsams.2020.10.007.
10. David Axe. (2024, 03 29). *Ground Assault Ended Badly ... For The Robots*. Retrieved from https://www.forbes.com/sites/davidaxe/2024/03/29/russias-first-ever-robotic-ground-assault-ended-badly--for-the-robots/?sh=4474d9e5435d

11. Dawinder S. Sidhu. (2007). The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans. *University of Maryland Law Journal of Race, Religion, and Class*, 377-392.
12. Dmitry Stefanovich. (2021). Russian hypersonic weapons: what, when and why? *International security, 04*, 78-80. Retrieved from https://www.researchgate.net/publication/354059412_Russian_hypersonic_weapons_what_when_and_why
13. Emma Helfrich. (2020, 10 20). *High Energy Laser weapon system in development with Boeing, General Atomics*. Retrieved from https://militaryembedded.com/radar-ew/sensors/high-energy-laser-weapon-system-in-development-with-boeing-general-atomics?gad_source=1&gclid=EAIaIQobChMI0JCiwte3hQMVhZGDBx2n7AFMEAMYASAAEgIZifD_BwE
14. Felix Lemmer. (2022, 05). Security Tech Brief: May 2022: Burevestnik. pp. 2-11.
15. IAEA. (2021). A Decade of Progress After the Fukushima Daiichi NPP Accident. *Proceedings of an International Conference Held in Vienna* (pp. 24-77). Vienna: Proceedings Series - International Atomic Energy Agency.
16. IAEA. (2024). *Fukushima Daiichi Nuclear Accident*. Retrieved from https://www.iaea.org/topics/response/fukushima-daiichi-nuclear-accident
17. Integrated Micro-Electronics. (2022, 12 05). *DIY Guns A Clear and Printed Danger*. Retrieved from https://www.global-imi.com/blog/diy-guns-clear-and-printed-danger
18. Jessica Katzenstein. (2023). *Total Information Awareness: The High Costs of Post-9/11 U.S. Mass Surveillance.* Watson Institute. Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://watson.brown.edu/costsofwar/files/cow/imce/papers/2023/Surveillance%2520Report%25202023%2520.pdf&ved=2ahUKEwiDy5bEuLKFAxWDgP0HHWUWAkYQFnoECCoQAQ&usg=AOvVaw07qIu7pwPGRVCDINAijk_R
19. Josef Taalbi. (2020). Evolution and structure of technological systems - An innovation output network. *Research Policy, 49*(8). doi: https://doi.org/10.1016/j.respol.2020.104010.
20. Kari Bingen, H. W. (2024, 04 02). *Russia's New Space Weapon.* Retrieved from https://www.youtube.com/watch?v=mmzRW5i6DDs
21. Kenedi, D. F. (2017). *Uzori hraborsti.* Albion books. (in Serbian)
22. Kyle Mizokami. (2024, 01 29). *Is the Aircraft Carrier Becoming Obsolete? Here Are 3 Ways We Could Replace Them*. Retrieved from https://www.popularmechanics.com/military/navy-ships/a46506473/are-aircraft-carriers-obsolete/
23. Leah Walker. (2020, 04). Nuclear-Powered Cruise Missiles: Burevestnik and its Implications. *Journal of Science Policy & Governance, 16*(1). Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/walker_jspg_v16.pdf&ved=2ahUKEwin6Yb2jbOFAxWw_rsIHU7AB5UQFnoECBAQAQ&usg=AOvVaw0Hg9HXItL3y5o3iQk8gfU_
24. Liav Orgad, W. R. (2020). *How to Make the Perfect Citizen? Lessons from China's Model of Social Credit System.* European University Institute. doi: ISSN 1028-3625
25. Mario Coccia. (2019). Theories of the evolution of technology based on processes of competitive substitution and multi-mode interaction between technologies. *Journal of Economics Bibliography, 6*(2), pp. 99-109. doi:10.1453/jeb.v6i2.1889.
26. McKay, H. (2023, 11 30). *A Look Inside Hamas's Weapons Arsenal*. Retrieved from The Cipher Brief All: https://www.thecipherbrief.com/a-look-inside-hamass-weapons-arsenal
27. NDTv. (2023, 10 16). *Video: Israel Recovers "Homemade" Weapons Used By Hamas As War Escalates*. Retrieved from https://www.ndtv.com/world-news/israeli-defence-forces-confiscates-hamas-grenades-rockets-and-medical-supplies-4484769
28. Özden ÖZKANLISOY, E. A. (2021). THE EFFECT OF SUEZ CANAL BLOCKAGE ON SUPPLY CHAINS. *MARITIME FACULTY JOURNAL, 14*(1), 51-79. doi:10.18613/deudfd.933816
29. Paul Schwartz, S. B. (2024, 04 04). *Innovations on the Battlefield in Ukraine with Paul Schwartz and Samuel Bendett.* Retrieved from https://www.youtube.com/watch?v=6m8t0JlihoU
30. Rae W. Archibald, J. J. (2002). *Security and Safety in Los Angeles High Rise Buildings After 9/11.* RAND. doi:https://doi.org/10.7249/DB381
31. Ragnar Benson. (1992). *Ragnar's Big book of homemade weapons.* Boulder, Colorado: Paladian Press. Retrieved from https://www.survivorlibrary.com/library/big-book-of-homemade-weapons.pdf

32. Rob A. Zuidwijk. (2021, 04 14). *Professor's Opinion - Suez Canal blockage*. Retrieved from https://www.rsm.nl/discovery/2021/opinion-suez-blockage/
33. Ryan Berg. (2023, 12 14). *Testify with Ryan Berg: Strengthening Energy Sanctions on Russia, Iran, and Venezuela.* Retrieved from https://www.youtube.com/watch?v=IWgvCIumZIU
34. Ryan C. Berg. (2023). *Restricting Rogue-State Revenue: Strengthening Energy Sanctions on Venezuela.* Washington DC: CSIS. Retrieved from https://www.csis.org/analysis/restricting-rogue-state-revenue-strengthening-energy-sanctions-venezuela
35. Tarraf, D. C. (2020). *An Experiment in Tactical Wargaming with Platforms Enabled by Artificial Intelligence.* Retrieved from https://www.rand.org/pubs/research_reports/RRA423-1.html.
36. TASS. (2023, 10 17). *Russia unveils ground-based combat robots fighting in Ukraine operation*. (TASS, RUSSIAN NEWS AGENCY) Retrieved from https://tass.com/defense/1692007
37. The Guardian. (2016, 03 14). *Homemade guns used in Palestinian attacks on Israelis*. Retrieved from https://www.theguardian.com/world/2016/mar/14/homemade-guns-carl-gustav-used-in-palestinian-attacks-on-israelis
38. Tim Kastelle, J. P. (2009). The evolution of innovation systems. *DRUID Summer Conference 2009.* Copenhagen: Copenhagen Business School.
39. Timothy Wright. (2023, 10 13). *Russia claims to have tested nuclear-powered cruise missile*. (IISS) Retrieved 04 08, 2024, from https://www.iiss.org/online-analysis/missile-dialogue-initiative/2023/10/russia-claims-to-have-tested-nuclear-powered-cruise-missile/
40. U.S. Naval Institute Staff. (2024). *Congressional Research Service report, Defense Primer: Navy Distributed Maritime Operations (DMO) Concept.* U.S. Naval Institute Staff. Retrieved from https://news.usni.org/2024/02/29/report-to-congress-on-navy-distributed-maritime-operations-concept
41. Warren Chin. (2019, 07). Technology, war and the state: past, present and future. *International Affairs, 95*(4), pp. 765–783. doi:https://doi.org/10.1093/ia/iiz106