M. Kubilay Akman

OPSEC Model and Applications

Security Dimensions. International & National Studies nr 1 (25), 60-81

2018

SECURITY DIMENSIONS
International & National Studies
NO. 25; 2018 (60–81)
DOI 10.24356/SD/25/3

OPSEC Model and Applications*

Assoc. Prof. Dr. M. Kubilay Akman, Ph.D.
Uşak University, TURKEY

ABSTRACT

OPSEC (Operations Security) model was developed during the Vietnam War era as a part of military strategies to protect critical information, analyzing vulnerabilities and threats, assessing risks and applying proper countermeasures. 5 steps OPSEC model have been functional for US Army's operational security and used by other NATO members as well. When threats have spread widely in 21 st Century OPSEC began to be used and applied in a more general context of security world. Today even in cyber security this model serves practically for protection of critical data and information. In this paper we are going to proceed in two levels: on the one hand we will explain the OPSEC principles, steps and conceptual aspects through the main sources of this field; on the other hand we will discuss applications of the model in real world (military, politics, industry, etc.) via some explanatory examples and its potential usages for securing modern life and societies. Our approach will be based on an interdisciplinary view with references to sociology, security studies and management.

ARTICLE INFO

Article history
Received: 12.12.2017 Accepted 05.02.2018

Key words
OPSEC, security studies, sociology of security, security management, information security, cyber security, risk society

* This paper is presented at Istanbul Security Conference 2017, http://istanbulguvenlikkonferansi.org/index.php/en/.

1. Introduction

Information is power when kept properly and may be cause of failure if it is not conducted and managed in the right way. Today information technologies and global networks enable risk factors to spread easier compare to previous eras of human history. Safety and security of a society cannot be maintained just by security personnel of a country. In accordance with law and human rights values all society and individuals need to take role for securing today and future of humanity.

Of course, we do not need to see just negative aspects of globalization and contemporary information technologies. At the beginning of 21st Century scholarly, scientific and academic interaction is in its highest level. This is a big advantage for universal human values and world peace. With ethical behaviors, globalization of knowledge can be helpful to improve life quality of societies internationally.

In defense and strategic studies, security sciences international exchange of knowledge has been effective always. For sure, thanks to contemporary translations and publications it is more in our age. Where is Sun Tzu read more, in the East or the West? The Chinese strategist and philosopher definitely very well known in the West. Western concepts of war, defense and strategy are researched, understood and applied in the East too. This is a very natural process and academic, intellectual and scientific progress is achieved by this way.

As a part of globalization of knowledge, scientific models and methodologies in this paper we will focus on OPSEC (Operations Security), a model designed and improved in the United States of America. Although the majority of researches on OPSEC has been conducted in the US, still there is a lot of aspects for its concepts to be analyzed, researched and discussed in other parts of the World. As all social sciences are becoming more international, same tendency is inevitable for security studies as well. OPSEC is also very suitable to emphasize interdisciplinary potential of security studies. In this paper we are going to follow an interdisciplinary perspective which is guided by a sociological approach. Because, insecurity and security are produced in societies, they are societal components and at the end of the day sociology is the science of society and anything related to societies.

2. What is OPSEC?

OPSEC, as an invention of last century, has been used very frequently besides military, security, intelligence, business, trade, etc. operations as a supportive model. It has become almost like an interdisciplinary subfield of security studies with several academies, schools, professional associations and educational programs. Before discussing its importance and potential to be functional in diverse dimensions of societies let us first give a definition of OPSEC. It can be defined as "an analytical process used to deny an adversary information (generally unclassified) concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations"[1]. As it is seen from the definition, for OPSEC it is very crucial to protect critical information of any institution's, organization's, department's plans, operations and intentions especially as keeping safe "unclassified" information.

OPSEC is a model which provides protection strategies in social life and communication. It is not considered merely as "a security, intelligence, or information assurance (IA) function"[2]. Intelligence is systematic coordination of activities which "provide information on adversary forces, governments, and intentions"; counterintelligence is performance of information gathering and conducting activities "to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities"[3]. OPSEC overlaps with these activities and they are mutually supporting each other. According to US military authorities "close coordination must be maintained between all staff functions to ensure adequate OPSEC protection"[4]. So, it can be said that although OPSEC is not an intelligence activity essentially its proper usage can be helpful to general intelligence strategies from many aspects. Furthermore, in 21st Century when we are talking about intelligence it is not just about official activities of all states, this is also highly connected to private activities of global or national com-

[1] COMDTINST M5510.24A, *Operations Security Program (OPSEC),* US Department of Homeland Security – United States Coast Guard, Washington DC 2014, p. 10.

[2] MCO 3070.2A, *The Marine Corps Operations Security (OPSEC) Program,* Department of the Navy, Washington DC 2013, p. 12.

[3] Ibidem.

[4] Ibidem.

panies as well, since corporate security and business intelligence have a growing importance in today's economy. So, OPSEC is a supportive model in private sector as well.

OPSEC's being "a process" is seen as its "most important characteristic" and "OPSEC is not a collection of specific rules and instructions that can be applied to every operation. It is a methodology that can be applied to any operation or activity for the purpose of denying critical information to an adversary"[5]. As a process it is very adaptable to different variations of operations with a suitable flexibility of principles. Its principles are not solid "rules" or "orders"; just a foundation which show where and how to focus.

***

The history of OPSEC was explained in one of classified NSA sources which has been partially unclassified later: *Purple Dragon: The Origin and Development of the United States OPSEC Program*[6]. US military, during its wars in Southeast Asia, particularly in Vietnam, had some serious defeats. Following these defeats an operation called Purple Dragon started and a professional team employed in this operation to investigate and research on reasons of failure. This operation showed that North Vietnam intelligence was finding the real intentions, plans and classified information of US forces through analyzing what is unclassified and available in open sources. Then, based on the research of Purple Dragon in 1966 and 1967 OPSEC concepts were designed[7]. In the following 50 years OPSEC has been more sophisticated, spread around all security departments and has gone beyond US borders and scope of state affairs.

3. The Structure

Adversaries may change according to organization, mission or context. Regardless the place it is applied OPSEC aims to give a possibility to look at to the picture from the perspective of potential adversary. As a practi-

[5] Joint Pub 3–54, *Joint Doctrine for Operations Security*, Department of the Navy, Washington DC 1997, p. I-1.

[6] NSA/CSSM 123–2, *Purple Dragon: The Origin and Development of the United States OPSEC Program*, "United States Cryptologic History: Series VI", 1993, The NSA Period, Vol. 2.

[7] Ibidem, p. 3–4.

cal tool it makes your understanding possible how your adversaries may grow their information about your organization and its activities. OPSEC concept provides an opportunity for threat analyses and create countermeasures for their prevention. As a living methodology it can be applied into any sector (state or private), operation, strategy and individual case. It is possible to be conducted in a very low-cost and can be seen as a "mindset" or "way of life"[8]. This simplicity and functionality have made the model's surviving possible for half a century.

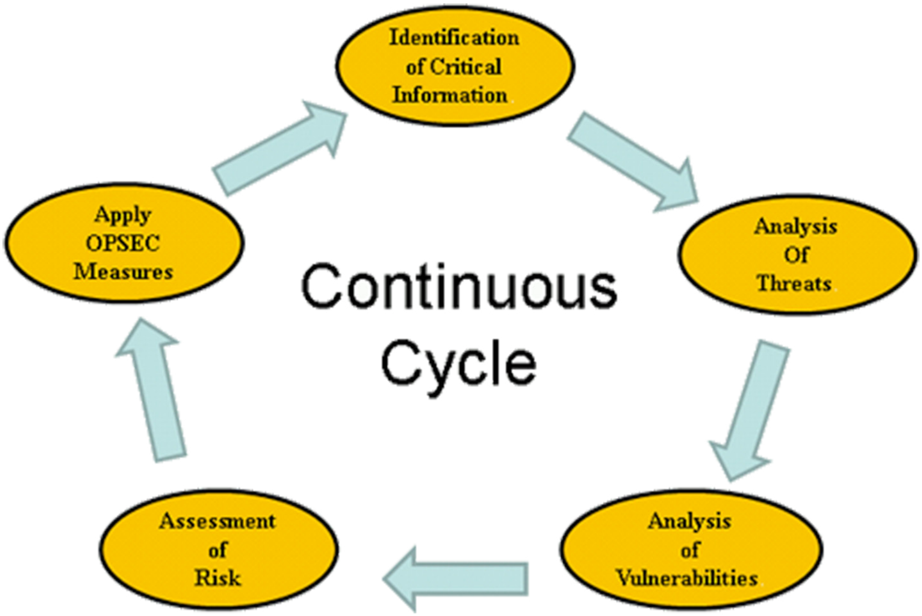


Image 1: OPSEC Cycle[9]

Federal Communications Commission (US) explains the steps of OPSEC model in business and IT context, although the essential principles and steps are the same for all sectors. An OPSEC process should follow 5 steps:
A. Identifying critical information.
B. Analyzing threats.

[8] OSPA, *Operations Security*, The Operations Security Professional's Association, 2009, www.opsecprofessionals.org, p. 6–9.

[9] Source: https://www.detrick.army.mil/ready/opsec/opsec03.cfm.

C. Analysis of vulnerabilities.
D. Risk assessment.
E. OPSEC countermeasures application[10].

These five steps or consecutive principles are the main framework of the model regardless it is used by military, police, intelligence, business or any other organizations. Different sectors or organizations may provide more or less some changing particularities. However, the model is structured on these five important points.

Each step of OPSEC has to be taken seriously for a successful operation. In case of failure in any level of this cycle all model would be weak and powerless for necessary measures. Now, let us have a look closer to these steps.

A. Identifying Critical Information

This is the first step in the OPSEC process and concepts. "In this step, critical information is identified by determining which information is critical to operations or desired by an adversary"[11]. Critical Information (CI), "if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, damage friendly resources, or cause loss of life"[12]. CI exist of some key information about "friendly activities or intentions that may significantly degrade mission effectiveness if revealed to an adversary. It should be noted, however, that information that is critical in one phase of the mission may not be critical in subsequent phases"[13]. So, for each case and context CI has to be defined separately.

B. Analyzing Threat

Understanding and analyzing capabilities of adversaries are the main points of the second step. By this way you can see that which kind of information they are looking for, who are your potential adversaries, how they try to get information, etc.[14] Adversaries' "collection activities target

[10] FCC, *Small Biz Cyber Planning Guide*, Federal Communications Commission, p. 1–2.

[11] OSPA…, p. 30.

[12] MCWP 3–40.9, *Operations Security (OPSEC)*, Department of the Navy, Washington DC 2009, p. 3–2.

[13] Ibidem.

[14] OSPA, *Operations Security…*, p. 31.

actions and open source information to obtain and exploit indicators that will negatively affect the mission"[15]. Relevant and updated information on threats "is critical in developing appropriate OPSEC protective measures. The threat assessment (TA) step in the OPSEC process includes identifying potential adversaries and their associated capabilities, limitations, and intentions to collect, analyze, and use knowledge of our CI against us"[16]. This step is crucial to go further and set effective solutions to security problems.

C. Analysis of Vulnerabilities

In third step you need to focus on your vulnerabilities. What are the vulnerable points of your organization? From where adversaries may give harm to your activities? These are essential questions for this analysis[17]. The aim with these questions and analysis "is to identify each vulnerability and draft tentative OPSEC measures addressing those vulnerabilities. The most desirable measures provide needed protection at the least amount of cost to operational effectiveness and efficiency"[18]. In military, security or business operations "Weaknesses that reveal CI through collected and analyzed indicators create vulnerabilities. Indicators are those friendly actions and information that adversary intelligence efforts can potentially detect or obtain and then interpret to derive friendly CI"[19]. When you can see your vulnerabilities clearly to arrange proper measures would be more possible and successful.

[15] III CORPS & FH REG 530–1, *Operations Security OPSEC Program,* Department of the Army, Fort Hood, TX 2017, p. 31.

[16] MCWP 3–40.9…, p. 3–3.

[17] OPSA…, p. 33.

[18] III CORPS & FH REG 530–1…, p. 31.

[19] MCWP 3–40.9…, p. 3–4.

Things Aren't Always As They Appear
Who's asking questions about your critical information?
You "DO" OPSEC
www.opsecprofessionals.org

Image 2: "Who's asking?" An OPSEC poster[20]

[20] Source: https://www.opsecprofessionals.org/opsec-posters.

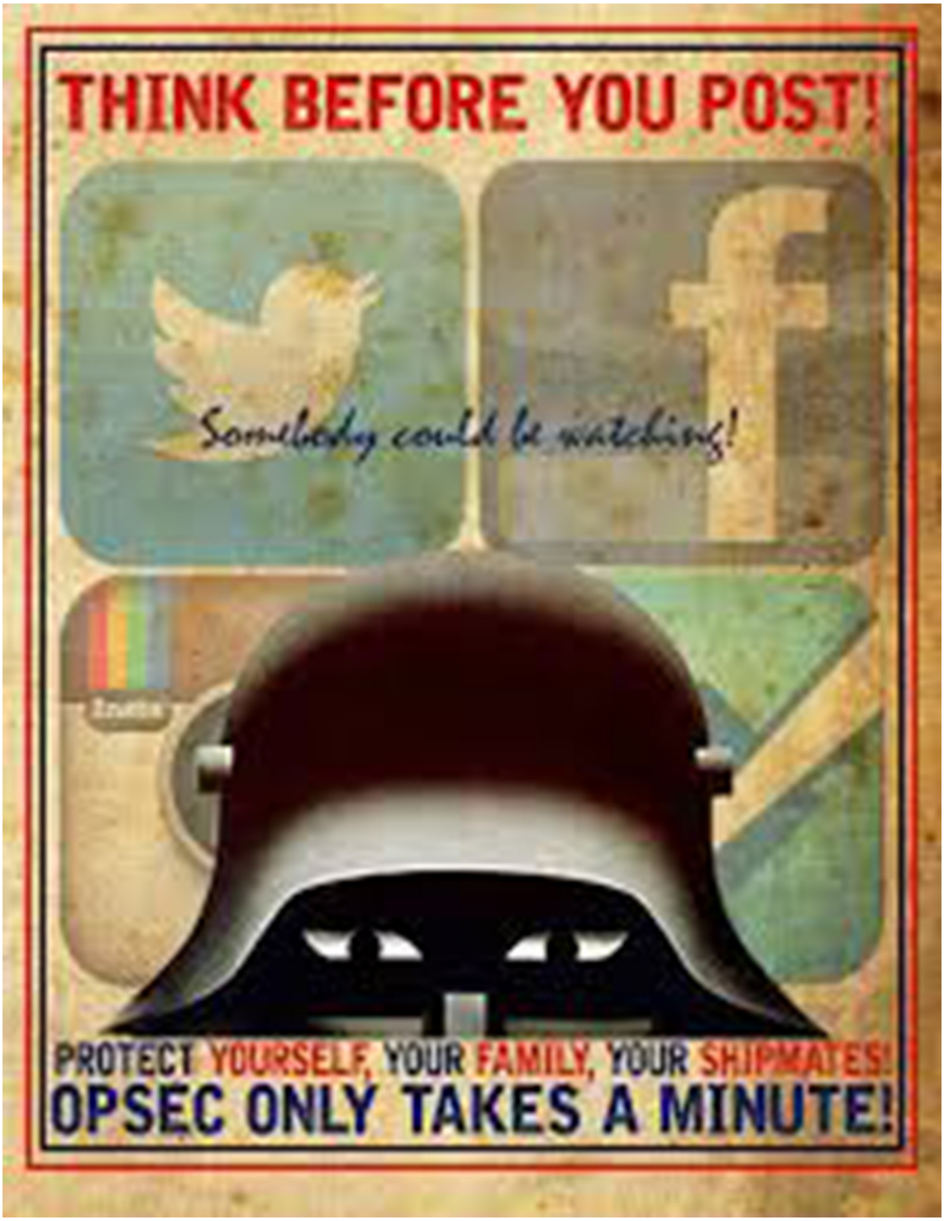
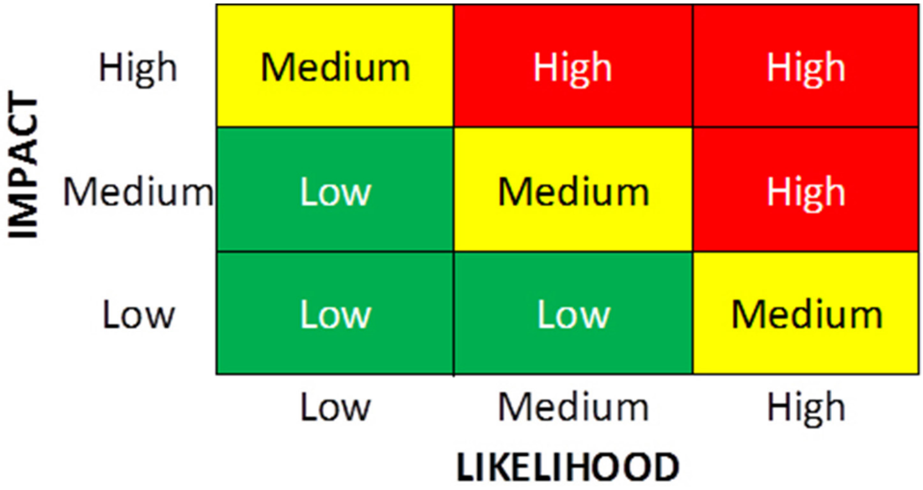

THINK BEFORE YOU POST!
Somebody could be watching!
PROTECT YOURSELF, YOUR FAMILY, YOUR SHIPMATES!
OPSEC ONLY TAKES A MINUTE!

Image 3: an OPSEC poster[21]

[21] Source: http://www.navy.mil/ah_online/OPSEC/posters.html.

D. Risk Assessment

After analyzing its vulnerabilities an organization needs to assess potential risks. OPSEC professionals, based on this risk assessment will decide what are needed effective countermeasures[22]. OPSEC concepts require "managing all dimensions of risk to maximize mission effectiveness and sustain readiness"[23]. This level has two important points: "First, OPSEC managers must analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Second, specific OPSEC measures must be selected for execution based upon a risk assessment done by your company's senior leadership"[24]. It is obvious that you cannot avoid from all risks, so "the risks have to be managed to an acceptable level"[25]. If the operation or mission continue successfully despite a threat or risk, then it would be much better not to create any complications with any measures. A risk assessment matrix would be helpful in order to understand what to apply in a particular situation.



IMPACT			
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium
	Low	Medium	High
		LIKELIHOOD	

Image 4: Risk Assessment Matrix[26]

[22] OPSA…, p. 34.

[23] MCWP 3–40.9, p. 3–5.

[24] FCC…, p. 2.

[25] III CORPS & FH REG 530–1…, p. 32.

[26] Source: https://www.pivotpointsecurity.com/blog/using-matrix-models-for-risk-assessment.

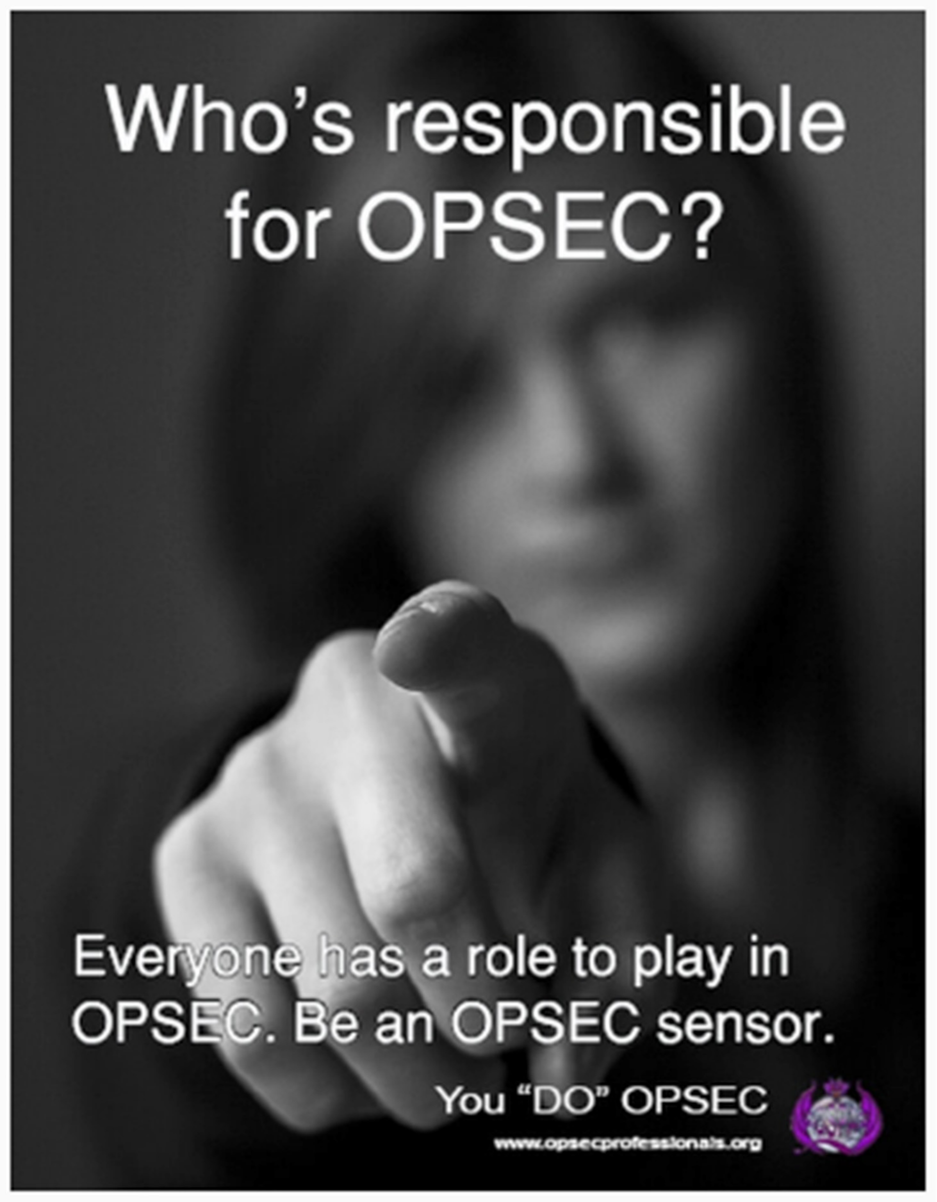

Who's responsible for OPSEC?
Everyone has a role to play in OPSEC. Be an OPSEC sensor.
You "DO" OPSEC
www.opsecprofessionals.org

Image 5: "Who's responsible?" An OPSEC poster[27]

[27] Source: https://www.opsecprofessionals.org/opsec-posters.

E. Applying Countermeasures

This can be named as the "action" step. In this final level the best solution is "a combination of low-cost countermeasures that afford the best security"[28]. OPSEC countermeasures emerge of three categories:

1. Prevention of adversaries from determining any indicators.
2. Using alternative and deceptive appearances of indicators.
3. Attacking adversaries' data collection systems and methods[29].

The application process of OPSEC countermeasures "is a continuous cycle that includes evaluating intelligence and counterintelligence reports, public media disclosures, website reviews, integrated systems security monitoring, feedback on reports such as assessments and surveys"[30]. As threats are continuous like a cycle countermeasures need to be the same way to be effective.

***

In contemporary societies "Our commercial, government, and academic enterprises are large organizations with many formal rules and regulations. Yet the essential workings of these enterprises are typically based on various social relations and unwritten rules"[31]. Any aspects and dimensions of social life are organized both through formal rules and unwritten norms, codes, values, customs, etc. at the same time. OPSEC is giving us an awareness and behavioral philosophies to keep our countries, societies, communities or companies safe and secure always.

21st Century has new challenges in security field; today "the nature and complexity of security threats is dynamically changing. The threats are less visible and more networked, which calls for a full set of new capabilities"[32] when security authorities are trying to create countermeasures. Terrorism, cybercrimes, violence, urban crimes, etc.; all kind of security threats are produced in societies and finding their environment for growth in societies as well. Responses to security threats have to be more general with a societal basis, beyond any particular security institution and organ-

[28] OPSA…, p. 36.

[29] MCWP 3–40.9…, p. 3–5.

[30] III CORPS & FH REG 530–1…, p. 33.

[31] A. Odlyzko, *Economics, Psychology, and Sociology of Security*, 2003, http://www.dtc.umn.edu/_odlyzko, p. 7.

[32] *Introduction to Security Studies*, Ondrejcsák R. (ed.),CENAA, Bratislava 2014, p. 235.

ization. OPSEC can be functional in this context, regardless its beginning historical context and origins in the US. We leave in a global world where knowledge and information cannot be taken in a monopoly and thanks to global sources any kind of technology, scientific knowledge or methodology are available to anyone seriously interested, of course unless it is protected with high measures of OPSEC.

After providing the concepts and methodological approaches of OPSEC we can have a look for examples which can be explanatory for understanding the philosophy and principles of Operations Security. An important point here, the chosen examples are not necessarily to be used before in OPSEC literature. Actually, original and new examples are more functional to comprehend the model properly. Another point, our examples are not limited to security field and other dimensions of societies are mentioned as well when it is helpful to our discussion. Crucial aim of this discussion is to show how OPSEC works (or could work) through successful cases and also avoidable failures. Common character of all our examples is that there is a pragmatic function: *explaining how OPSEC philosophy to operate in real life experience and field*[33].

4. Cases and Facts

Regarding the power of OPSEC or failure with its lack can be understood through several cases from 20th and 21st centuries. Sometimes, tangible facts can be more clear and understandable than theoretical explanations. Let us focus on the cases:

A. Iranian Revolution

Interestingly the Iranian Islamic Revolution (1979) happened after the OPSEC concept is developed by the US military and intelligence authorities. It can be said that Islamic revolutionaries used some elements of the philosophy of OPSEC against the USA and its allies unintentionally.

Gary Sick, who was from Jimmy Carter's National Security Council claimed that "the United Stated had scaled back its intelligence gathering inside Iran in the lead-up to the revolution in deference to the Shah, which helped contribute to U.S. officials overlooking widespread Iranian resentment against the Shah and the United States and underestimating

[33] All cases are selected regardless whether the actors refer to OPSEC. Because, for us it is important if context is suitable for the model.

the ability of the religious opposition to overthrow the Shah"[34]. So it can be said that Ayatollah Khomeini and his followers kept their critical information safe and meantime they obtained the critical information of the Shah power. On the other hand, the US failed about vulnerabilities analysis and risk assessment. As a result of this failed and unsuccessful OPSEC picture the Iranian Revolution has had victory. Strategically and in terms of OPSEC philosophy and principles Ayatollah Khomeini was very successful.

Image 6: Iranian Revolution[35]

B. Wikileaks

Australian citizen Julian Assange founded Wikileaks in 2006 and started to publish classified information of governments. As a philosophical basis he has claimed that they are against authoritarian politics which are in his opinion based on "secrecy" and related conspiracies. So,

[34] U. Friedman, *The Ten Biggest American Intelligence Failures*, "Foreign Policy", 2012, http://foreignpolicy.com/2012/01/03/the-ten-biggest-american-intelligence-failures.

[35] Source: https://news.nationalgeographic.com/news/2009/06/photogalleries/iran-protest-david-burnett-pictures/photo2.html.

Wikileaks started to publish thousands of serious diplomatic documents in collaboration with several news agencies and newspapers as well[36]. Wikileaks has shown that how it can be damaging if critical information cannot be protected properly.

Image 7: Wikileaks logo

C. Poor OPSEC in Automotive Industry

Volkswagen company was accused in 1993 about "industrial espionage after Jose Ignacio Lopez, the chief of production for GM's Opel division, left to join the rival German automaker, along with seven other executives. GM claimed its corporate secrets were used at VW. In the end, the companies agreed to one of the largest settlements of its kind: GM would drop its lawsuits in exchange for VW's pledge to buy $1 billion of GM

[36] J. Zittrain, M. Sauter, *Everything You Need to Know About Wikileaks*, MIT Technology Review, 2010, https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks.

parts over seven years. In addition, VW was to pay GM $100 million"[37]. The lack of OPSEC principles is the main reason of this scandal.

Image 8: Volkswagen Company Headquarters[38]

D. Sharp Edge of Industrial Espionage

An engineer worked with Gillette company, who was in the team of a new shaver system project, gave confidential information of the company to the competitors in 1997: "Steven Louis Davis, an employee at Wright Industries Inc., a designer of fabrication equipment that was hired by Gillette, faxed or e-mailed drawings of the new razor design to Warner-Lambert, Bic, and American Safety Razor. Davis pled guilty to theft of trade secrets and wire fraud and was sentenced to 27 months in prison. He told the court he stole the information out of anger at his supervisor and fear for his job"[39]. Gillette's not applying OPSEC properly gave company a big security trouble.

As we can see from the last two examples OPSEC is a necessity for corporate security strategies as well. It should not be considered only a part of national defense. Where there is a critical information to protect there is a place for application of OPSEC model.

[37] https://www.bloomberg.com/news/photo-essays/2011–09–20/famous-cases-of-cor porate-espionage.

[38] Source: http://myautoworld.com/brand/volkswagen.

[39] https://www.bloomberg.com/news/photo-essays/2011–09–20/famous-cases-of-cor porate-espionage.

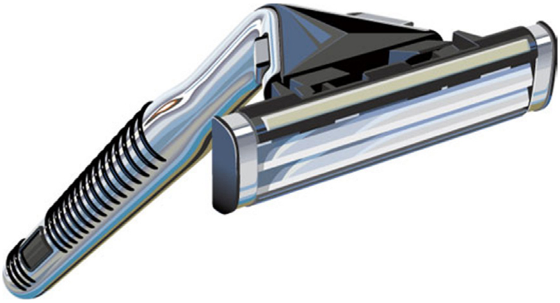


Image 9[40]

E. The Battle of Kursk

The final example can be from military history. During World War II German troops attacked to Russian army, as supposing that their number and power are less than their own army. German military authorities underestimated Soviet power because of a deception concept called *Maskirovka* used by Russian military intelligence. It has actually a common point with OPSEC as its main purpose is protecting the critical information (CI), in this case the huge amount of Russian troops, weapons and armed soldiers. Of course if the German knew that they would not attack at all to Russia.

Image 10: P. Krivonogov, *The Battle of Kursk*, painting[41]

[40] Source: http://www.plstudio.biz/product-rendering/product-closeup-razor.html (This razor just used as a sample of industrial design, nothing to do with the case).

[41] Source: http://www.allworldwars.com/Soviet War Paintings.html.

German army did not realize that the actual power of Russians was four times higher than them. The Battle of Kursk (1943) started with the offensive actions of the German. Russia spread among Russian soldiers rumors what they want to be known as information by the German army and this information is transferred by German counterintelligence. They also hided their important military assets, constructed fake airfields and dummy aircrafts. When these were attacked the German military supposed that they are winning. As a result of *Maskirovka* (military deception) doctrine Russians were the winner of the Battle of Kursk[42]. This battle was a critical step and after this Germany became defensive in Eastern front.

***

Sociology is the main discipline which focus on society and besides it there are other disciplines as well which's subject is also society: economics, political sciences, management, anthropology, history, etc. Contemporary sociology provides us opportunities to study society with its all components; "The study of interactions, institutions, methods of socialization and processes of change forms a whole which can be defined as the study of society"[43]. Alain Touraine indicates that today there is a question on sociology arises: "can we redefine the sphere of sociology or must we admit that its days are now numbered and that new intellectual approaches must replace that of sociology"[44]. Answer of this question depends on how kind of sociologist you are. If we are flexible enough and open to "innovative approaches" in our discipline, then there is still a functional value of sociology.

Modern life is full of risks in many different layers of societal dimensions. In contemporary sociology Ulrich Beck has been the name who provided "the theory of risk society". According to Beck the "explanatory theory" of risk society "must include the institutional conditions, consequences, contradictions and the resulting dynamic of the new era, define the meaning of new practical experiences and throw light upon the interrelation between historical change and lifeworld experiences and practices"[45]. Modern society is producing the risk elements of contemporary

[42] J. H. Kantor, *10 Amazing And Successful Military Deception Operations*, 2016, https://listverse.com/2016/06/27/10-amazing-and-successful-military-deception-operations.

[43] A. Touraine, *Sociology without Societies*, "Current Sociology", 2003, Vol. 51 (2), p. 123.

[44] Ibidem, p. 126.

[45] U. Beck, *Critical Theory of World Risk Society: A Cosmopolitan Vision*, "Constellations", 2009, Vol. 16, No 1, p. 16.

life every day. According to Ulrich Beck contemporary societies are manufacturing uncertainties and insecurities: “Manufactured uncertainties are those kinds of risks that emerged as answers to the uncertainties introduced by modernity. They produce a wide range of risks. And science, even good science, even the best science, is always producing numerous alternative risks”[46]. This can be seen in IT sector, medicine, internet, chemistry, industry, etc. Each progressive step creates a new potential risk.

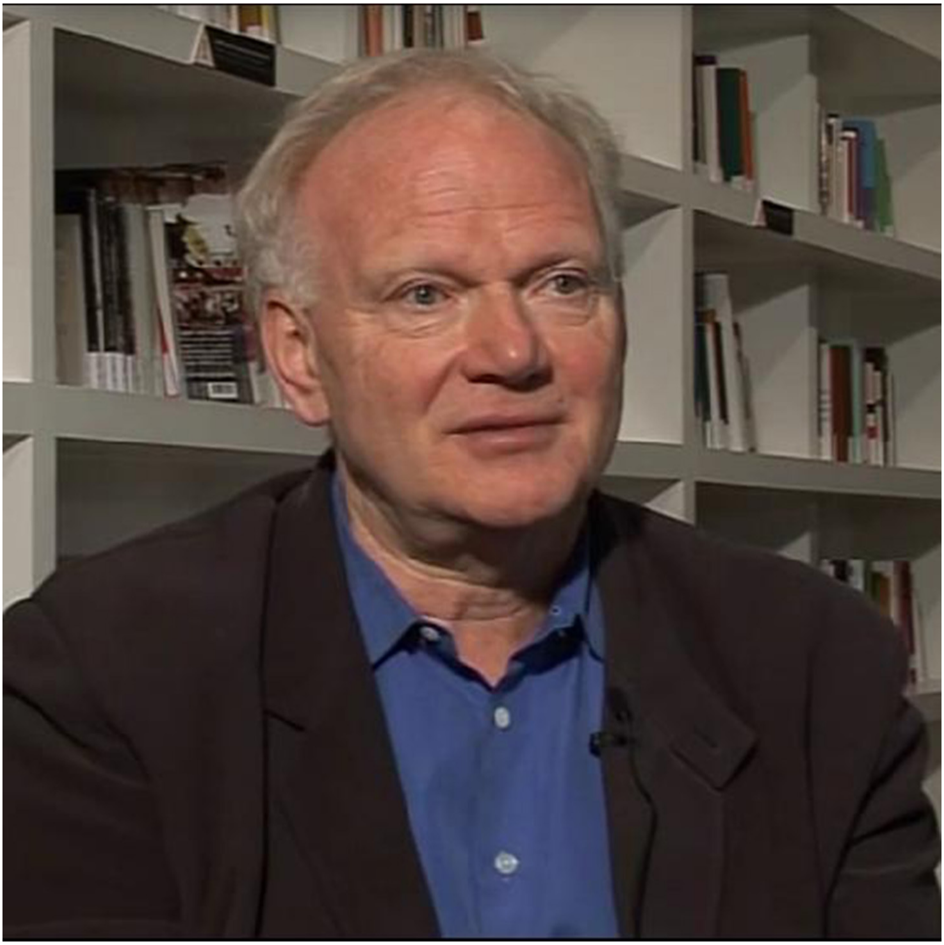


Image 11: Ulrich Beck

[46] L. Culver and others, *Revisiting Risk Society / A Conversation with Ulrich Beck,* RCC Perspectives, Munich 2011, p. 8.

Ulrich Beck emphasized that "ontological insecurity" of risk society drives modern individual into a crisis: "the recipient of the residual risk of the world risk society is the individual. Whatever propels risk and makes it uncalculable, whatever provokes the institutional crisis at the level of the governing regime and the markets shifts the ultimate decision-making responsibility onto the individuals who are ultimately left to their own devices with their partial and biased knowledge, with undecidability and multiple layers of uncertainty"[47]. The individual, as the final "decision-making" actor needs to go beyond "their own devices with their partial and biased knowledge" which would contribute undecidability and uncertainty further[48]. OPSEC, in this context, can be functional to create a secure environment, without any uncertainty and indecision. With the philosophy and principles of OPSEC an individual may figure out how to react and handle any situation in case of a security risk. Practicality, functionality, compatibility and simplicity of OPSEC are biggest advantages to apply it in modern risk society. When a person knows how to behave and how to set countermeasures against any potential risk she / he would feel less confused as an actor with "decision-making responsibility". OPSEC is the interdisciplinary social-technology applicable for social institutions and their security problems in 21st Century.

5. Conclusion

We have seen in this paper how OPSEC model and its steps are working. The CI (Critical Information) is more important, OPSEC needs to be more advanced and comprehensively conducted. Five steps of the model are explained in accordance with its philosophy and concepts. The example cases have given us the opportunity to see how OPSEC principles may be applied in security situations and if it is not used as a protective way how kind of damages and dangers can be confronted. OPSEC already has completed a half century lifetime. What will happen to it, if it will progress and improve further or replaced by other models and concepts will be seen by the time. As for now, it is a topic of security studies which waits to be discussed and researched from different perspectives and approaches internationally.

[47] U. Beck, *Critical Theory…*, p. 9.

[48] Ibidem.

References

1. Beck U., *Critical Theory of World Risk Society: A Cosmopolitan Vision*, "Constellations", 2009, Vol. 16, No 1.
2. COMDTINST M5510.24A, *Operations Security Program (OPSEC),* US Department of Homeland Security – United States Coast Guard, Washington DC 2014.
3. Culver L. and others, *Revisiting Risk Society / A Conversation with Ulrich Beck,* RCC Perspectives, Munich 2011.
4. III CORPS & FH REG 530–1, *Operations Security OPSEC Program,* Department of the Army, Fort Hood, TX 2017.
5. FCC, *Small Biz Cyber Planning Guide*, Federal Communications Commission.
6. Friedman U., *The Ten Biggest American Intelligence Failures*, "Foreign Policy", 2012, http://foreignpolicy.com/2012/01/03/the-ten-biggest-american-intelligence-failures.
7. Joint Pub 3–54, *Joint Doctrine for Operations Security*, Department of the Navy, Washington DC 1997.
8. Kantor J. H., *10 Amazing And Successful Military Deception Operations*, 2016, https://listverse.com/2016/06/27/10-amazing-and-successful-military-deception-operations.
9. MCO 3070.2A, *The Marine Corps Operations Security (OPSEC) Program,* Department of the Navy, Washington DC 2013.
10. MCWP 3–40.9, *Operations Security (OPSEC)*, Department of the Navy, Washington DC 2009.
11. NSA/CSSM 123–2, *Purple Dragon: The Origin and Development of the United States OPSEC Program*, "United States Cryptologic History: Series VI", 1993, The NSA Period, Vol. 2.
12. Odlyzko A., *Economics, Psychology, and Sociology of Security*, 2003, http://www.dtc.umn.edu/_odlyzko.
13. *Introduction to Security Studies,* Ondrejcsák R. (ed.),CENAA, Bratislava 2014.
14. OSPA, *Operations Security*, The Operations Security Professional's Association, 2009, www.opsecprofessionals.org.
15. Touraine A., *Sociology without Societies*, "Current Sociology", 2003, Vol. 51 (2).

16. Zittrain J., Sauter M., *Everything You Need to Know About Wikileaks*, MIT Technology Review, 2010, https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks.

Author

M. Kubilay Akman – sociologist and academic from Turkey. Head of the Sociology Department, University of Uşak**.**

Cite this article as:

M. Kubilay Akman, *OPSEC Model and Applications*, “Security Dimensions. International and National Studies”, 2018, no 25, p. 60–81, DOI 10.24356/SD/25/3.