SCENTIA INTERNATIONAL ECONOMIC REVIEW
Volume 1 - Issue 1 - 2021

Applying DEFCON and the Homeland Security Advisory System in organisational risk management

Benjamin Bendel, Comenius University, Bratislava, Slovakia
Jochen Schwenk, Comenius University, Bratislava, Slovakia
Tom Madsen, Comenius University, Bratislava, Slovakia
Milan Fekete, Comenius University, Bratislava, Slovakia

Abstract

Many businesses face avoidable strategic and external risks that can be addressed by accepting, relocating, reducing, or eliminating them. Companies of all sizes should predict and prepare for the risks that come with doing business. When a scenario becomes a reality, a well-prepared organisation can mitigate sales, lost time and productivity, and negative impact on customers. They can assist in the safety of an organisation and its employees by offering a fully integrated threat management system that offers real-time threat impact assessments that the corporation can use to fulfil its duty of care obligations and keep employees safe. These systems are based on robust systems such as DEFCON, HSAS, and NTAS. In analogy to the application in Military and Anti-Terrorism, the systems DEFCON, HSAS or NTAS to the specific application, define the comprehensive explanations and define corresponding actions at each threat level. This article deals with the question, if the deployment of DEFCON, HSAS/NTAS is a suitable approach to meet the requirements of the ISO 9001:2015. To answer the given research-question the method of qualitative content analysis was used as outlined by Mayring. Six main codes and twelve subcodes were defined inductively and deductively, and the present literature was encoded according to the method of structured content analysis. To this end, 765 codings were carried out and then analysed in the context of the research questions. As a result, the research question was confirmed by the present study.

Keywords: Organisational risk, Risk management strategies, DEFCON, HSAS, NTAS
JEL Codes: D00, L00

1. Introduction

Threats of all kinds are permanently affecting businesses, and it is important to interested stakeholders constantly track and analyse the risks. This is also important to satisfy the ISO 9001:2015 criteria. The risks to any organization are various. General threats such as politics, war, natural disasters, blackouts, and pandemics are continuously escalating. Caused by those general events there are numerous risks on a less global scale: disrupted supply chains, commercial or legal issues, even personal problems by key shareholders - just to name a few. Every organisation must continually assess these risks, and emergency preparation must be implemented before any occurrence and adapted as needed. Running a company entails a variety of risks. Some of these possible threats can completely kill a business, while others can cause significant damage that is both expensive and time-consuming to fix. Many companies face preventable strategic and external risks that can be dealt with by embracing, moving, reducing, or removing them. Regardless of the inherent risks of doing business, companies of all sizes should expect and plan for them. A well-prepared company will reduce the effects on revenue, lost time and efficiency, and negative impact on consumers when a possibility becomes a reality (Bishop et al. 2010, p. 115). Recognising risks is an important aspect of strategic business planning for both start-ups and existing businesses. Identifying these risks necessitates a thorough examination of a company's particular business practises. The complexities of safeguarding a modern workforce necessitate modern solutions (Bishop et al. 2010, p. 123). They can help protect an enterprise and its workers by providing a fully integrated threat management system that provides real-time threat effect assessments that the company can use to meet its duty of care obligations and keep employees safe.

Emergency communications capabilities are integrated into modern threat control systems. They help an organisation collect threat information and segment the audience to only include the affected employees (Bishop et al. 2010, p. 135). The approach saves the company time and increases the probability of a successful result. It also helps it conduct health tests, collect information about current employee needs, and communicate risks to any size audience. These systems are based on robust systems such as DEFCON, HSAS, and NTAS. The defence readiness condition (DEFCON) is a warning status used by the United States armed forces. The Homeland Security Advisory System (HSAS) uses a similar system. The article's emphasis is on the empirical issue of whether the DEFCON and Homeland Security Advisory Systems can be changed to meet the needs of companies' warning states in various economic circumstances.

The slowness with which HSAS provided usable information was one of the issues that led to its replacement by the National Terrorism Advisory System (NTAS). In the world of corporate security, speedy real-time notifications are extremely critical because they enable clients to rapidly address any problems that could threaten their facility or employees (Reese 2005, p. 7). When security alerts are provided in real-time to a customer and their security vendor, the two will work together to find the best solution (Reese 2005, p. 11). Real-time monitoring allows a minor incident to be resolved before it becomes a significant one, enabling security professionals and their clients to fix issues (Reese 2005, p. 13) easily.

Clients will feel more secure knowing that they will obtain a report as soon as a serious issue occurs (Reese 2005, p. 14). Most importantly, as information is exchanged more openly, this increased openness creates trust between the customer and their security provider.

Managing risk is not the same as managing policy. The emphasis on risk management is on the negative. It goes against the can-do attitude that most leadership teams strive for when executing strategy (Wang, Yang & Zhou 2019, p. 04067). Many leaders have a propensity to discount the future, and they are slow to invest time and money now to prevent an unknown future issue (Wang, Yang & Zhou 2019, p. 04067). Furthermore, risk mitigation usually entails dispersing capital and diversifying assets, the polar opposite of an effective strategy's concentrated emphasis (Wang, Yang & Zhou 2019, p. 04067). Managers can find it counter-cultural to endorse processes that recognise risks to the strategies they helped to create.

Therefore, companies need a separate role to handle strategy and external risk. The risk role's size can vary by organisation, but it must report directly to the executive team. The most important role would undoubtedly be to maintain a strong relationship with senior leadership. HSAS, DEFCON, and other exclusive threat reduction programmes, on the other hand, failed miserably because they overlooked the value of keeping the American public informed about threats.

2. Methods

Literature research identified 521 potential sources, 67 of which were identified as relevant sources. All sources which met the generally valid scientific requirement of the level of detail and the quality of the preparation were considered relevant. 20 primary sources were used in this work. These are mainly recent works with a release date of later than 2000. The latest work is the journal article from Wang et al. 2019.

This literature was encoded with the MaxQDA software. For this purpose, 6 main codes and 12 subcodes were defined inductively and deductively, and the present literature was encoded according to the method of structured content analysis. To this end, 765 codings were carried out and then analysed in the context of the research questions. The method of qualitative content analysis was used as outlined by Mayring to answer the following research question:

‘Is the deployment of DEFCON, HSAS/NTAS also a suitable approach to meet the requirements of the ISO 9001:2015?’.

3. Results

In this section the results of the qualitative data analysis are presented.

3.1 The Defence Readiness Condition

The United States Armed Forces use the defence readiness condition (DEFCON) as an alert state. The Joint Chiefs of Staff (JCS) and unified and specified combatant commands created the DEFCON framework, which prescribes five levels of readiness for the US military (Critchlow 2006, p.1). It goes from DEFCON 5, which represents the least extreme, to DEFCON 1, which represents the most severe, to reflect various military situations. DEFCON is a subsystem of an alert system that often includes Emergency Conditions (EMERGCONs) (Critchlow 2006, p.2). The Chairman of the Joint Chiefs of Staff and the Combatant Commanders are in charge of the DEFCON level, which is largely managed by the US President and Secretary of Defence (Critchlow 2006, p.4). For the staff in question, each level determines essential protection, activation, and response scenarios.

In different security situations, different branches of the US Armed Forces and different bases or command units may be activated. In general, there is no single DEFCON status for the entire world or any given region, and it can be limited to particular geographic areas (Hersman 2020, p. 1). Many commands have different defence readiness requirements, which have evolved, and the US Department of Defense refers to DEFCON levels during exercises using exercise terminology (Hersman 2020, p. 2). This is to prevent any misunderstanding between exercise commands and real operational commands.

The Cold War prompted the creation of DEFCON. In this war without major battlefield actions, the United States aimed all of its nuclear bombs at Moscow, and Russia was doing the same towards Washington (Wang, Hong & Chen 2012, p. 3323). The Air Force responded to the need of the cold war presented by founding the North American Aerospace Defence Command (NORAD) in 1958 to provide early warning and defence against nuclear threats (Wang, Hong & Chen 2012, p. 3329). NORAD proposed the DEFCON system in 1959, but it has evolved. It developed a warning system, each with comprehensive explanations and military actions anticipated at each threat level (Wang, Hong & Chen 2012, p. 3321). In November 1959, the JCS specified the DEFCON scheme for military commands, with Alpha and Bravo conditions under DEFCON 3 and Charlie and Delta conditions under DEFCON 4 (Wang, Hong & Chen 2012, p. 3335). It also had an Emergency level higher than DEFCON 1, with the two conditions of Defence Emergency and Air Defence Emergency.

DEFCON 5 is the military's standard level of readiness during times of peace. As a result, military planning and operations begin as a normal feature. Security protocols in this level are basic, with all personnel accessing every military base being subjected to ID checks (Woolf 2016, p. 2). This degree of defence, like all others, is currently in effect across the US until the Department of Defence changes it. The US military does not take any additional precautionary safety steps than are usually needed at DEFCON 5. This level does not always

imply that the world is at peace since conflicts, even major ones, can erupt all over the world during a DEFCON 5 (Woolf 2016, p. 2). On the other hand, the military believes that these incidents pose no major security risks in this situation.

DEFCON 4 is the next degree of intensity, with enhanced intelligence collection and security measures. There are more staff on guard at all hours of the day and night and random inspections of vehicles entering a military base (Woolf 2016, p. 3). Also, more staff are added to guard those areas that were not staffed during level 5. DEFCON 4 is not always a sign that the military or the country is in danger of being attacked. It is thought that this level is often released after small to moderate terrorist acts and politically motivated killings or after would-be plots are discovered in the modern world (Woolf 2016, p. 4). This is most likely being done in preparation for more attacks, to plan for and deter them.

DEFCON 3 refers to circumstances in which the United States or its allies might be subjected to military action. The Air Force can deploy in 15 minutes at the DEFCON 3 level of military readiness (Woolf 2016, p. 5). With the addition of security staff, base activities become substantially altered. All necessary Air Force personnel are on high alert at military bases and ready to prepare and deploy (Woolf 2016, p. 5). Furthermore, based on classified protocols, all military communications can be encrypted. DEFCON 3 has traditionally been associated with circumstances in which military aggression against the United States or one of its allies was a distinct possibility (Woolf 2016, p. 5). All military personnel must also remain within fifty miles of their operational base under this condition. Commanders have the authority to order all of their staff to stay on base.

DEFCON 2 is just below the highest degree of severity. A level 2 upgrade is severe, and all combat units must be ready to deploy within 6 hours (Woolf 2016, p. 6). This situation raises the possibility of primary military operations against the US or its allies. Except in the most militarily tense of international environments, DEFCON 2 is usually reserved. The most famous instance of DEFCON 2 was during the Cuban Missile Crisis, though this declaration was only given to Strategic Air Command (Woolf 2016, p. 6). Since DEFCON-related information is normally kept confidential, this is the first time in US history that a wide-scale DEFCON 2 warning has been released.

Both military personnel are kept ready for immediate action in DEFCON 1, the highest level of readiness. This suggests that a full-fledged war is on the horizon. Military personnel begin to deploy at this stage (Woolf 2016, p. 7). There is a possibility that nuclear weapons could be used against the United States or its allies. While, as previously mentioned, DEFCON levels are typically kept secret until after the fact, it is believed that DEFCON 1 has never been given to a branch of the US military (Woolf 2016, p. 7). However, certain military sections might have been stationed at DEFCON 1 during the Gulf War crisis.

3.2 The Homeland Security Advisory System

In March 2002, President Bush signed Homeland Security Presidential Directive 3, which established the Homeland Security Advisory System (HSAS). According to Behunin (2004, p. 1), this was part of a series of initiatives to strengthen coordination and cooperation among all government and the American public in the fight against terrorism. The advisory framework laid the groundwork for establishing a robust and efficient communications mechanism for disseminating information about the threat of terrorist threats to all government levels and the general public in the United States (Behunin 2004, p. 4). HSAS was created to warn federal, state, and local government agencies and the general public about the danger of terrorist attacks (Behunin 2004, p. 5). HSAS was a colour-coded terrorism threat advisory scale (Behunin 2004, p. 5). Its various levels prompted detailed responses from federal agencies and state and local governments, and they had an effect on security at certain airports and other public locations.

HSAS was handed over to the current Department of Homeland Security (DHS) when the department was formed in January 2003. The Secretary of Homeland Security, in consultation with the Assistant to the President for Homeland Security, determines whether to publicly announce threat conditions (Ganderton, Brookshire, & Bernknopf 2004, p.8). Inspired by the forest fire colour system's success, the scale consists of five color-coded threat levels, which were intended to reflect the probability of a terrorist attack and its potential gravity. Red symbolises severe risk, orange high risk, yellow significant risk, blue general risk, while green symbolises low risk (Ganderton, Brookshire, & Bernknopf 2004, p.9). The intensity coding makes identification and response easier.

While the government had given general instructions to citizens and federal agencies, the precise government behaviour, caused by instances where various threat levels were not always revealed to the public, caused public mistrust. Increased police and other security presence at landmarks and other high-profile locations, increased surveillance of international borders and other entry points, ensuring that emergency response services were ready (Reese 2005, p. 2). In some instances, deployment of members of the National Guard and State Guard to assist local law enforcement on security information were all actions taken previously (Reese 2005, p. 3). The Fourth Amendment to the United States Constitution was used to challenge some of the acts taken as a result of the threat rate stipulated in HSAS.

There were no published threat level guidelines, so there was no way to know if the current threat level was correct according to the knowledge available for the public. According to Shapiro & Cohen (2007, p. 121), supporters of the framework justified this by claiming that disclosing detailed, current intelligence about terror groups will jeopardise the ability to collect similar data in the future. Some critics were concerned that the lack of clearly identified, objective standards had resulted in the baseline threat level being set as elevated,

preventing the system from ever being reduced to low or general (Shapiro & Cohen 2007, p. 131). As a result, the system's communicative meaning and choices were limited to the three highest values (Shapiro & Cohen 2007, p. 134). The framework was also prone to government officials' exploitation due to the lack of transparency.

With time, federal, state, and local government agencies were worried about whether they are obtaining the requisite information to respond adequately to heightened warnings. They were also worried about the potential costs associated with preventive measures (Sharp 2013, p. 1). Congress recommended that the US analyse HSAS's operations (Sharp 2013, p. 2). The Homeland Security Advisory Council voted in December 2004 to review the color-coded scheme (Sharp 2013, p. 6). On April 27, 2011, the system was replaced by a new system known as the National Terrorism Advisory System.

3.3 The National Terrorism Advisory System

The color-coded HSAS was replaced by the National Terrorism Advisory System. According to Sharp (2013, p. 8), this new framework was created to efficiently convey information about terrorist threats to the public, government departments, first responders, airports, and other transportation hubs, and the private sector in a timely and comprehensive manner. It acknowledged that all Americans share responsibility for the country's security and that everyone should be aware of the increased risk of a terrorist attack in the United States and what they should do in the event of one (Sharp 2013, p. 11). The Department of Homeland Security uses bulletins in NTAS to disseminate information about developments and non-specific risks. There are three types of alerts, and these are elevated, intermediate, and imminent.

When DHS has details about a real, credible threat, it releases a formal warning with as much detail as possible. When a public warning is issued, it provides information on the geographic area, critical infrastructure that the threat may impact, mode of transportation, steps individuals or communities may take to protect themselves and their families, and preventive measures taken by authorities (Shapiro & Cohen 2007, p. 144). It also lays out the steps to follow in the event of a specific terrorist attack. Individual threat warnings are sent out for a set period, after which they immediately expire, and they can be expanded if new information becomes available (Shapiro & Cohen 2007, p. 154). The public is informed whether the hazard has been extended or is about to expire in the same manner that the initial notification was made.

3.4 Preventive Risk Management

Risk management is the process of identifying, analysing, and responding to risk factors that arise throughout a company's operations. Effective risk management entails trying to influence potential results as much as possible by behaving proactively rather than reactively (Thun & Hoenig 2011, p. 242). As a result, good risk management can reduce both

the likelihood of a risk happening and the effects of that risk. Structures for risk management are designed to do more than just identify existing risks (Thun & Hoenig 2011, p. 245). A good risk management structure should also quantify and forecast the effect of uncertainties on a company. Thus, a business must choose between accepting threats and dismissing them (Thun & Hoenig 2011, p. 249). Threat acceptance or rejection is determined by the tolerance levels that a company has set for itself.

Risk management structures may be used to help other risk reduction programmes if they are established as a disciplined and continuous mechanism to identify and address risks. Planning, organisation, expense control, and budgeting are among these structures (Tsiokanos et al. 2020, p. 1121). Since the emphasis is on constructive risk management, the company is unlikely to face many surprises in this situation. A company must use a problem-solving approach when building contingencies (Tsiokanos et al. 2020, p. 1126). Since it can deal with risks as soon as they emerge, such a strategy would allow a business organisation to deal with obstacles or blockages to its progress.

Risk assessment is a required method because it provides a company with the resources it needs to identify and handle potential risks properly. Risk management also gives a company a solid foundation for making sound decisions (Peek-Asa et al. 2017, p. 940). Risk evaluation and management are the best ways for a company to plan for events that may obstruct progress and development (Peek-Asa et al. 2017, p. 944). When a company reviews its strategy for dealing with future threats and then establishes mechanisms to deal with them, it increases its chances of being successful (Peek-Asa et al. 2017, p. 950). Progressive risk management ensures that high-priority risks are addressed as quickly as possible.

Applying DEFCON, HSAS, and NTAS in Preventive Risk Management

Threat detection and mitigation models focus their operating processes on business threat identification and mitigation models. The business must be informed as soon as the device detects a relevant threat (Mattern et al. 2014, p. 702. Thus, a business can use the modalities provided in national alert systems like DEFCON, HSAS, and NTAS to create effective strategies for threat assessment and management. Threat identification and mitigation processes are emphasized in DEFCON, HSAS, and NTAS. In turn, these elaborate systems can be used to mitigate threats quickly and efficiently.

To fill a global threat database, modern threat management systems use several sources where threat information is vetted and compiled by expert analysts and trusted content sources (Ali, Al Lawati & Naqvi 2012, p. 176). This helps the company cut through the noise and provide actionable, timely content that it can use to handle potentially damaging situations. Threat data must provide an evaluation of the threat's effect on the company to be genuinely useful. With remote and moving workers spread worldwide and new threats arising regularly, an organisation requires assistance in assessing the possibility of threats that could affect the company (Kuligowski & Dootson 2018, p. 1). Advanced threat management systems can compare real-time location data from employees to threats from around the world, determining the danger to the organisation (Kuligowski & Dootson 2018, p. 3).

However, on a more specific level, a business can implement a system similar to DEFCON, HSAS or NTAS for the complete organisation or limited to certain organisational structures, e.g., departments, or operational fields, e.g., the supply chain or maintenance of critical infrastructure of the business. The aim is to adapt the systems DEFCON, HSAS or NTAS to the specific application, define the comprehensive explanations and define corresponding actions at each threat level. A single, accountable employee with managerial authority should be named (Olsson 2006, p. 4). Members of a risk management committee can be assigned particular duties and must report to the risk manager (Olsson 2006, p. 6).

4. Conclusion

According to the requirement of the ISO 9001:2015, all risks must be handled on two levels. All risks identified in the entity have to identified, merged, controlled, and checked. Risk orientation on the operational level must be part of the value chain. Criteria have to be defined based upon the probability of occurrence of adverse events and the resulting amount of damage. Requirement is also to prioritise within clearly defined clusters. First step is to catalogue risks, also including the interaction between single risks and cumulated single risks that could lead to a global risk. Based upon this assessment, counteractions have to be defined, implemented, and controlled. In conclusion, the deployment of DEFCON, HSAS/NTAS is also a suitable approach to meet the pertinent requirements of the ISO 9001:2015. Future research on this topic must empirically investigate the possible civilian implementation of DEFCON, HSAS/NTAS in detail and thus elucidate further existing blind spots. In addition, the numerous possible fields of application and possible critical undesirable developments should be precisely defined and also critically empirically examined.

References

Ali, S, Al Lawati, M, H, & Naqvi, S, J 2012, 'Unified threat management system approach for securing SME's network infrastructure.' In *2012 IEEE Ninth International Conference on e-Business Engineering* (pp. 170-176), IEEE.

Behunin, S, A 2004, 'Homeland Security Advisory System.' *Naval Postgraduate School Monterey CA Dept of National Security Affairs*.

Bishop, M, Engle, S, Frincke, D, A, Gates, C, Greitzer, F, L, Peisert, S, & Whalen, S 2010, 'A risk management approach to the "insider threat".' In *Insider Threats in Cyber Security* (pp. 115-137). Springer, Boston, MA.

Carter, A, B 1985, 'The command and control of nuclear war.' *Scientific American*, vol. 252, no. 1, pp.32-39.

Critchlow, R, D 2006, 'Nuclear command and control: Current programs and issues.' *Library of Congress Washington DC Congressional Research Service*.

Ganderton, P, T, Brookshire, D, S, & Bernknopf, R, L 2004, 'Improving the Homeland Security Advisory System: An experimental analysis of threat communication for national security.' *Library of Congress Washington DC Congressional Research Service*.

Hersman, R 2020, Wormhole escalation in the new nuclear age (Summer 2020).' *Texas National Security Review*.

Kuligowski, E, & Dootson, P 2018, 'Emergency notification: Warnings and alerts.' *Encyclopedia of wildfires and wildland-urban interface (WUI) fires*.

Mattern, T, Felker, J, Borum, R, & Bamford, G 2014, 'Operational levels of cyber intelligence.' *International Journal of Intelligence and Counterintelligence*, vol. 27, no. 4, pp.702-719.

Nolte, W, & Kruse, R 2011, 'Readiness level proliferation.' *Air Force Research Laboratory, Air Force Research Laboratory, Tech. Rep. 88ABW-2011-5501*.

Olsson, F 2006, 'Intrusion Management.' *Rapporter från MSI*

Peek-Asa, C, Casteel, C, Rugala, E, Holbrook, C, Bixler, D, & Ramirez, M 2017, 'The threat management assessment and response model: A conceptual plan for threat management and training.' *Security Journal*, vol. 30, no. 3, pp.940-950.

Reese, S 2005, 'Homeland Security Advisory System: Possible issues for congressional oversight.' *Library of Congress Washington DC Congressional Research Service.*

Shapiro, J, N, & Cohen, D, K 2007, 'Color bind: Lessons from the failed homeland security advisory system.' *International Security*, vol. 32, no. 2, pp.121-154.

Sharp, V, H 2013, 'Faded Colors: From the Homeland Security Advisory System (HSAS) to the National Terrorism Advisory System (NTAS).' *Naval Postgraduate School Monterey CA Dept of National Security Affairs*.

Thun, J, H, & Hoenig, D 2011, 'An empirical analysis of supply chain risk management in the German automotive industry.' *International journal of production economics*, vol. 131, no. 1, pp.242-249.

Tsiokanos, I, Mukhanov, L, Georgakoudis, G, Nikolopoulos, D, S, & Karakonstantis, G 2020, 'DEFCON: generating and detecting failure-prone instruction sequences via

stochastic search.' In *2020 Design, Automation & Test in Europe Conference & Exhibition* (pp. 1121-1126), IEEE.

Wang, S, Hong, L, & Chen, X 2012, 'Vulnerability analysis of interdependent infrastructure systems: A methodological framework.' *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 11, pp.3323-3335.

Wang, Y, Yang, M, & Zhou, X 2019, 'The path selection model of emergency logistics based on cumulative prospect theory.' In *E3S Web of Conferences* (Vol. 136, p. 04067), EDP Sciences.

Woolf, A, F 2016, 'Defense primer: Command and control of nuclear forces.' *Congressional Research Service.*