DOI: https://doi.org/10.33865/JSSGP.8.01.220

2023
JOURNAL OF SECURITY STUDIES AND GLOBAL POLITICS
Volume:8 www.sciplatform.com Issue: 1
ISSN (Online) 2519-9609

SWOT Analysis and Security Management

Muhammad Kubilay Akman
Sociology Department of Uşak University, Turkey.

SWOT analysis is an analytical method used in management to understand strengths, weaknesses, opportunities and threats of an organization. It has been used widely since 1960s. Conventional management literature has references to SWOT frequently. However, in security management this method is not used sufficiently. In this article we will have an opportunity to discuss details of SWOT and its applicability to security management field as well. Security managers can benefit from SWOT besides other analytical methods and tools. Internal and external aspects of companies and organizations are evolving very fast. SWOT may provide us a chance to see the potential tendencies in internal and external levels.

Key word: SWOT analysis, security management, sociology of security, business administration, security studies, corporate security.

Author(s) Contributions	**M. K. Akman:** conducted all the study and wrote manuscript.

*Corresponding email address: kubilayakman@gmail.com

INTRODUCTION

Security management is not an easy task. There are prolific, transforming and growing threats in contemporary world. Security managers must be aware and alert facing all these threats. To see what is present today is not enough: they have to see future's trends, changing and evolving nature of risks as well. We are going to discuss SWOT analysis in this article. What can be the advantages we may obtain through the analytical steps of SWOT? In business world this method has been used since 1960s. However, there is a gap in academic literature about security management and SWOT. We will try to ask some preliminary questions regarding functionality and usefulness of SWOT analyses in security management processes. Internal and external factors, challenges and potentials are important aspects for security managers to evaluate and comprehensively analyze. What does make your organization strong or weak, what are positive and negative possibilities around you? Security authorities, like all other managers, need to see and understand these points while conducting their tasks. Therefore, general management methods and tools (including SWOT) are also highly usable for security managers as well. Managing a security team and securing a business require to understand these concepts properly.

SWOT concepts: SWOT is the abbreviation of "Strengths, Weaknesses, Opportunities and Threats". Any organization seeking effective solutions and powerful strategies for their operations may use SWOT with their own approaches and interpretations based on particular needs and environments. SWOT analysis' standardized application "is based on a template, which provides the necessary heuristics to examine the future prospects of an organization. This investigation is structured in terms of potential that may promote, or barriers that may hinder, the achievement of the organization's goals (Hovardas, 2015). Where are located our power and weaknesses, how kind of threats and opportunities we will face are major questions in SWOT (figure 1).

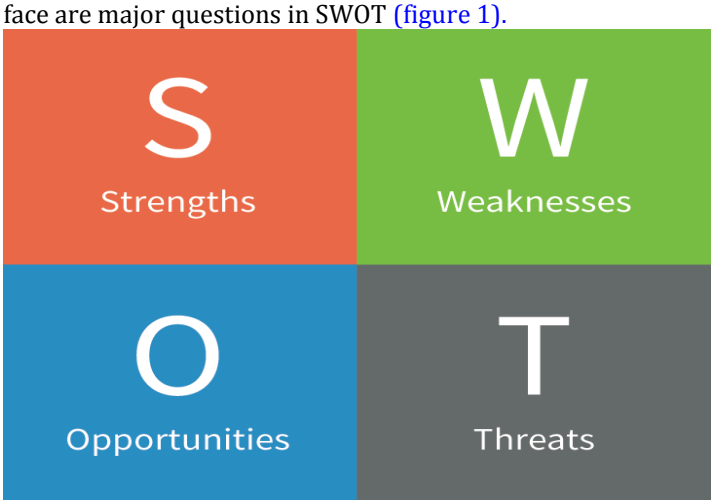


Figure 1: SWOT Model (Hildeman, 2015)

Classical way of SWOT requires "the detailed identification and classification of all phenomena and states affecting the development of the system"; and there are two criteria in this procedure: "The first is the nature of the effect of actual or potential impact of a factor to the organization, while the second – the wider location factor in terms of organization. The use of these two criteria can distinguish four groups of factors: strengths and weaknesses as well as opportunities and threats" (Nazarko, 2017). These four corners of SWOT give us the possibility of maintaining successful strategies for our organization, regardless educational, private, political, governmental, NGO, Etc.

As an analysis and decision making model SWOT has "internal and external factors". When we understand both dimensions of organization we can have a whole picture of potentials, risks, possibilities and disadvantages.

Internal factors: S (strengths) letter and W (weaknesses)

indicate "internal factors", i.e. your available "resources and experience". Following factors are covered in this part: Financial resources, physical resources / facilities, human factor / personnel, natural resources, patent and copyrights, brands, existing processes (organizational, structural, IT, Etc.).

External factors: External factors are represented with letters of O (opportunities) and T (threats). External influences (regardless opportunity or threat) "affect every company, organization and individual"; therefore we should focus on them. These factors "typically reference things you or your company do not control", for instance: trends of market, tendencies in economy, demographics, relations with business partners, regulations and conditions in politics, environment and economy (Fallon, 2008). These factors are located outside of the organization with huge influence to inside mechanisms either directly or indirectly (figure 2).

Figure 2: SWOT Analysis

The separation between internal and external factors is based on the distinction "between the characteristics of the organization itself and the elements which are attributed to the organization's environment". From this perspective "the organization's potential to accomplish its objectives is judged against both inner (i.e., that pertain to the organization itself) as well as outer (i.e., environmental) aspects that may be mobilized in order to accomplish the goals of the organization" (Hovardas, 2015). "Strengths" and "weaknesses" are considered as inner aspects, as for "opportunities" and "threats" emerge as outer aspects to the company. From this dual (inside / outside) view barriers can be found either in the organization or in the surrounding environment (Hovardas, 2015). SWOT analysis provides "insights concerning the trajectory of the organization categorized in 'strengths' that should be supported (i.e., inner potential), 'opportunities' that have to be sought (i.e., environmental prospects), 'weaknesses' that must be overcome (i.e., inner barriers), and 'threats' that ought to be alleviated (i.e., environmental hindrances)" (Hovardas, 2015). When supported with other managerial tools SWOT can be functional for establishing strategic directions and overcoming internal and external difficulties of organizations.

Andrzej Sztando has proposed an "extended SWOT analysis" which is named as SWOT Plus. His model is designed "according to method of strategic analysis of local government territorial entities" (Nazarko, 2017) and he mentioned eight factors in the extended model of SWOT:

1. **Strengths:** These are the properties (active or inactive) in the system,
2. **Weaknesses:** Existing system properties which function as barriers to development,
3. **Internal opportunities:** Opportunities which have high effect and coming from internal structure of organization system,
4. **Internal threats:** Existing however inactive properties of the system which brake its development,
5. **Stimulants:** External factors (active) contribute to the system's development,
6. **Counter stimuli:** External active barriers which brake the system's development,
7. **External opportunities:** Positive external factors,
8. **External threats:** – Negative external factors (Nazarko, 2017).

As we may see SWOT Plus is an extension of classical SWOT to respond the more complicated nature and requirements of contemporary systems and organizations. This is an improvement of the classical model.

It is better to know that although it is widely used in public or private sectors and diverse fields there are also critiques against SWOT among management scholars or professionals. It is criticized as having "shallow theoretical roots" and claimed it runs "no deeper than the tenet that, like any living organism, a business can prosper only if it achieves a good fit between itself and its environment" (Valentin, 2005). There are strong critiques and rejections against SWOT such as: "Typical SWOT guidelines promote superficial scanning and impromptu categorizing in lieu of methodical inquiry. The SWOT framework does not readily accommodate tradeoffs. SWOT guidelines commonly muddle accomplishments and strengths. SWOT guidelines generally lack criteria for prioritizing SWOTs. Hence, items are listed as if all were equally important, and critical matters often are obscured by clutter" (Valentin, 2005). Of course, we cannot say that all factors are equal (internal, external, potential or active); if SWOT analysis is not done comprehensively its benefits would be arguable.

Another critique to SWOT is that "by exploring the weaknesses and threats", emphasizing these negative aspects "organizations often cause more harm than good. More than an avoidable pothole or roadblock, gaping canyons and immovable mountains emerge, giving way to downward-spiraling feelings of hopelessness and fear. These conversations, stemming from repeated analysis of what's wrong or missing, highlight awareness around what isn't desired, which carries little momentum to inspire compelling visions of a most desired future" (Silbert, 2007). This problem can be especially harmful to the psychological balance and harmony of staff among themselves and in relation with the environment. It is better to consider and apply SWOT analysis

in equanimity rather than to see it as a "magic wand".

Security environment and challenges for today's businesses: In contemporary business world companies are mostly nervous about threats against IT. Twelve major threats can be mentioned although there are more in fact: syndicates of cybercrime, money launderers, hacktivists, corporate espionage, mercenaries of malware, spyware, ransomware, all-in-one malware, compromised web, cyber warfare, shadow IT, software vulnerabilities (Grimes, 2017; Baker, 2017). Of course in information society and global economy IT-related threats are very important and can be severely harmful. However, more physical and on-site threats are also existing in different parts of the world ranging from terrorism to insurgencies and conflict, from street gangs to more sophisticated and veiled criminal networks of the elite. Therefore, understanding security environment, not only on business level, also in societal and human dimensions are crucial for maintaining successful security management in 21st century.

What is security? When we look at constructivists they have a common tendency "in their commitment to avoiding universal and abstract analytical definitions of security" (McDonald, 2008). However, "the central shared assumption of constructivist approaches to security is that security is a social construction" (McDonald, 2008). Actually, their approach is partially correct, considering the wide diversity of human populations, societies and socio-political, socio-economic systems; it is not easy to have a universal concept of security. On the other hand, in order to be able to communicate scientifically we need to have a sound definition of "security" although this will not make constructivists or neo-constructivists happy. We may suggest a definition such as: "security is the total picture and includes fractional entities of all social interactions, *praxis* and constructions which are organized, produced, reproduced, performed and conveyed intersubjectively for maintaining a secure social environment for continuation of related social, societal and human activities / operations". Economy and business are perfectly covered in this scope since these activities are parts of society and humanity.

Capitalism does not have a clean history. However, in contemporary world awareness of societies, social groups and individuals have limited the previous greed of capitalist economy. Today "human values", ecological sensitivities and peaceful approaches are more dominant than ever in the history of homo sapiens. For contemporary security actors every day increasingly "humanistic" view is having further importance in their practices in security environment. Before discussing human aspects, especially in the frame of "human security" concept, let us analyze security environment and its dimensions.

When we analyze "security environment" this analysis "assesses the specific dimensions of social environment with focus on security and creates space for the analysis the processes running within and serves for the identification of threats and dangers, as well as of actors" (Ušiak, 2014). Analyzing security environment is necessary for both public and private, military or civilian security specialists. Knowing in which kind of environment security operations are run is essential for effective security administration or security management. Regardless related security actors are soldiers, police, other government agents or corporate security officers always a comprehensive analysis is necessary. Security environment "includes several analytical levels, by which we can approach the assessment of actors in the security environment: International systems (global), which comprise mutually interacting and depending units without any superior level, are determined by major trends, including globalization, uneven development, demographic factors and new generation of threats and dangers (terrorism, proliferation of light arms and WMD, international organized crime, narcotics-related activities, money laundering, and so on)" (Ušiak, 2014). The threats mentioned here are as much harmful as cyber threats to businesses. Terrorism, organized crime, proliferation of arms, Etc. can create real troubles to security managers of companies too. So, these are not only problems of the military, law enforcement and intelligence agencies.

Security environment has "global, continental, regional, local, and individual" levels of existence, like circles inside each other but sometimes not limited with the lines of particular circle. When "the various types of security environment" are formulated "the criticism of analytical levels is based especially on an impossibility to accurately define the actors of particular levels" (Ušiak, 2014). We can try to define a security actor in a level but s/he or it can switch to another level (or circle), it is a flowing process.

Security challenges of contemporary world are creating a complicated security environment. Therefore, "There is a need for organizations, leaders, and individuals to adapt to an increase in the type and intensity of stressors and ambiguity existing in today's business, political, and defense environments, a need that is not limited by organizational or generational boundaries" (Gallagher, 2013). Security measures of organizations, institution, leaders and other charged individuals have to be as dynamic and flowing as today's actual threats in security environment.

Private companies of security take more responsibility in contemporary global environment and "provide military and security services to states, international organizations, NGOs, global corporations and wealthy individuals" (Avant, 2008). This is a reality of 21st century. This reality has contributed to widening the scope and definition of security: Although in a contestation period realists tried "to maintain the 'narrow' definition, now there were to be a variety of referents for security – society, humanity, the individual – as well as the state, and a variety of sectors of security – economic, political, societal, environmental – to go alongside the military" (Croft, 2008). Private security companies and security managers of corporate world should remember these issues, especially

points related to humanitiy's core values (figure 3).

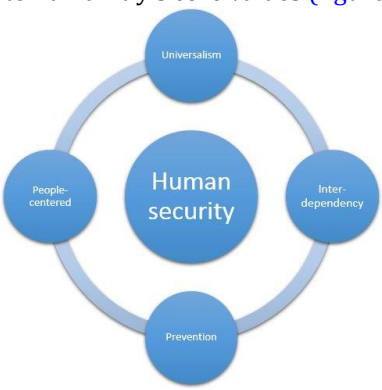


Figure 3: Human Security

Human security is discussed more and more every day in academia. How to define it? "One way is to define it negatively, i.e. as the absence of threats to various core human values, including the most basic human value, the physical safety of the individual"; another way is "a more positive definition of human security: 'The objective of human security is to safeguard the vital core of all human lives from critical pervasive threats, and to do so without impeding long-term human flourishing.'" (Hampson, 2008). In the Commission on Human Security's report there is a "more expansive" definition: "to protect the vital core of all human freedoms and human fulfilment" (Hampson, 2008). Human security has the meaning of "protecting fundamental freedoms. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military, and cultural systems that together give people the building blocks of survival" (Hampson, 2008). This is really an expansive definition. Maintaining a human security policy for the benefit of the earth and all world people requires also private sector's security management actors to take responsibility. This cannot be only the role of governments and public authorities. It is the right time for an effective security management to focus and care about human values as well. If security actors look at to humanity and its values with sulky faces this can be only the precursor of an upcoming dystopia.

When we discuss below the SWOT concepts for an effective security management we should always consider that in both location for companies (internal and external) there is "humanity". It is better always keep in mind a humanistic approach in security analyses and practices.

Effective security management: Security management is an essential discipline for continuity of businesses which has a lot common with management sciences and security studies field in general. For an effective security management responsible authorities/directors have to maintain a harmonious combination between security concerns and management perspectives for this purpose.

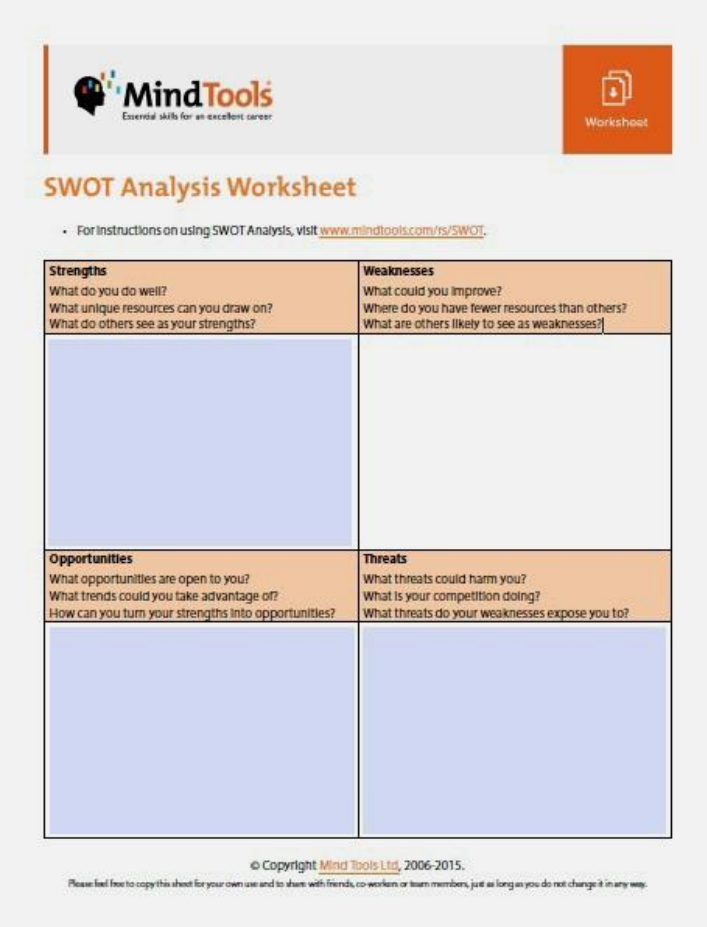
Security management is a complex process "for today's businesses and corporations". A CSO (Chief Security Officer) "is charged with identifying the organization's assets then overseeing the documentation, development and implementation of any necessary policies/procedures for the protection of those assets. The CSO's responsibilities may be divided into four basic categories: Information Security and Audits, Security Basics, Physical Security and Business Continuity, and Security Leadership." These tasks require adequate knowledge and skills both in management and security fields.

SWOT analysis may be highly functional for effective and powerful security management strategies when taken and applied properly. It can provide "a good foundation for your strategy, business proposition, the position of your company, the direction of your company, and even discover which ideas are worth pursuing"; and "SWOT is simple, and can be completed by every business and organizations" (Fine, 2009). This works also for security management activities and can be used by CSOs or other levels of security profession.

The general benefits of SWOT analysis are also helpful for CSOs in security management processes. It gives "opportunities of "collaboration on strategic plan formulation"; incorporating "many different internal and external factors"; maintains a "structured process that allows for a thorough idea gathering"; "The posting of the ideas vs. the yelling minimizes the reactionary processing and group mentality from occurring"; in decision making process "participants who may traditionally be quiet and participate less, are encouraged, and have the ability to participate" more productively; allows the ability for a more equalized and interactive communication; in management "responses are prioritized within each category, by importance, giving units a clearer understanding of their most pertinent topics and areas to address". SWOT can help to realize a substantial communication in stressful work environment of security.

CSOs and other security management authorities can use a worksheet for conducting SWOT analysis. The worksheet may exist of four parts to include: strengths, weaknesses, opportunities, threats. In the section of "strengths" there can be some questions such as "What do we do best? What resources can we draw on? What do other parties perceive as our strengths?" We can type our answers on the worksheet or if necessary to extra pages. We should reflect on these strong parts of our company, organization, service. What makes us stronger is our power for successful strategy and operations. It is advisable, if the legal procedure allows, not publicize this and also other parts of SWOT Analysis. It is not a smart idea to show your opponents where you have strength and weakness (figure 4). Better to follow "invisibility" principles of Ninpo (Ninjutsu, Ninja arts and way).

In the square for weaknesses we can ask what can we improve, where do we have less resources, what are



MindTools
Essential skills for an excellent career

Worksheet

SWOT Analysis Worksheet

- For instructions on using SWOT Analysis, visit www.mindtools.com/rs/SWOT.

Strengths	Weaknesses
What do you do well? What unique resources can you draw on? What do others see as your strengths?	What could you improve? Where do you have fewer resources than others? What are others likely to see as weaknesses?
Opportunities	**Threats**
What opportunities are open to you? What trends could you take advantage of? How can you turn your strengths into opportunities?	What threats could harm you? What is your competition doing? What threats do your weaknesses expose you to?

Figure 4: SWOT Worksheet (MindTools)

weaknesses other people see in us? These are really important questions. If as a security leader you do not know where is your organization is weak there may be most probably where you will be harmed. It is better to diagnose and correct it as soon as possible. In a very advanced way of strategy you can use your weakness as a tool of deception in competition. However, this is beyond the scope of this article.

After strengths and weaknesses, in the next two parts we should cover the external elements, opportunities and threats for our organization or company. There are particular questions to be answered in these parts of our SWOT worksheet. With your answers you will be more aware of opportunities and threats. The questions are about what opportunities you have in presence, in which trends you could take advantage, what are the ways to transform your strengths to opportunities? What kind of threats can give harm to your organization? What are your competitors doing? Considering your weaknesses, in which ways you can be more vulnerable? When all your answers are visible on a worksheet it is technically more manageable and easier to comprehend general view at one sight. Of course this cannot take the place of all complicated researches and reports. But, sometimes the simplest techniques can give you a picture which makes possible to organize your mindset properly. In arts, literature, science, management and many other fields masters have frequently more plain, sometime even primitive sketches you never see. What you see is the result, a masterpiece. This is the same for security management. Methods, techniques, practical steps do not matter; what you will achieve is matter actually.

SWOT analysis is a method of management and a tool widely used by directors, managers in the process of creating strategies. It has been used commonly "as a tool for the analysis of internal and external factors in order to achieve a systematic approach and support to address the situation." When we look at contemporary business world "Internal and external factors are the most important for the future of businesses. They are called strategic factors and are presented in the SWOT matrix. The ultimate goal of the strategic planning process, of which the SWOT is one of the initial phases, is development and adoption of strategy resulting in a good relationship between the internal and external factors" (Oreski, 2012). SWOT analysis provides effective analytical functions to security managers regarding how to maintain secure, safe and sustainable business activities. In security strategy planning they can use SWOT to understand internal and external factors, their interactions and possible tendencies towards future.

CONCLUSION

Modern world is not only marked with quantitative increase of security challenges, it has been also characterized through qualitative transformation and complication of threats in societies. There are risks contemporary organizations, businesses, global companies facing which are entirely different than previous ages. This great level of change necessitates a comprehensive approach to set measures.

As we have seen in this article SWOT analysis is a functional method to understand internal and external aspects of organizations. CSOs (Chief Security Officers) can use this tool to see strong and weak dimensions of their companies in terms of security. They can focus to maintain countermeasures based on seeing what are actual threats and opportunities. SWOT model can be modified in accordance with particular needs of your company. Ensuring its functionality is more important than observing strict steps of the method. When confronting dynamic problems security leaders need effective tools, SWOT analysis is one of them. It is useful, practical and relevant. This is the reason why it is still used after a half century.

REFERENCES

Avant, Deborah D. (2008), "Private Security", in (Williams, 2008)

Baker, Steven (2017), "5 Types of IT Security Threats Facing Businesses", Rutter, https://www.rutter-net.com/blog/5-types-of-it-security-threats-facing- businesses Accessed: 05. 05. 2019

Croft, Stuart (2008), "What Future for Security Studies?", in (Williams, 2008)

Fallon, Nicole (2008), "SWOT Analysis: What It Is and When to

Use It", March 2, 2018, https://www.businessnewsdaily.com/4245-swot-analysis. html Accessed: 01.05.2019
Fine, Lawrence G. (2009), The SWOT Analysis, Kick It, LLC, http://www.lawrencefine.com
Gallagher, Shane (2013), "Transforming Education through Neuroscience, Cognition, and Game Design", in (Wells, 2013)
Grimes, Roger A. (2017), "IT's 9 biggest security threats", CSO, https://www.csoonline.com/article/3215111/security-it-s-9-biggest-security-threats.html Accessed: 05.05.2019
Hampson, Fen Osler (2008), "Human Security", in (Williams, 2008)
Hildeman, Greg (2015), "Using SWOT Analysis to Plan an Uncertain Future and Increase Organizational Effectiveness", https://nexightgroup.com/using-swot -analysis-to-plan-an-uncertain-future-and-increase-organizational-effectiveness Accessed: 01.05.2019
Hovardas, Tasos (2015), "Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis: A template for addressing the social dimension in the study of socioscientific issues", AEJES, 1
McDonald, Matt (2008), "Constructivism", in (Williams, 2008)
MindTools, "SWOT Analysis Worksheet", http://www.mindtools.com/rs/SWOT Accessed: 25.06.2019
Nazarko, Joanicjusz, Ejdys, Joanna and others (2017), "Application of Enhanced SWOT Analysis in the Future-oriented Public Management of Technology", Procedia Engineering 182
OIEA, SWOT Manual, Austin Community College
Oreski, Dijana (2012), "Strategy development by using SWOT - AHP", TEM Journal, Volume 1, Number 4
Ondrejcsák, Robert (Ed.) (2014), Introduction to Security Studies, Centre for European and North Atlantic Affairs (CENAA), Bratislava
Silbert, Jen Hetzel & Silbert, Tıny (2007), "SOARing from SWOT: Four Lessons Every Strategic Plan Must Know", Innovation Partners International
Ušiak, Jaroslav (2014), "Introduction to Security Studies", in (Ondrejcsák, 2014)
Valentin, Erhard K. (2005), "Away With SWOT Analysis: Use Defensive/Offensive Evaluation Instead", The Journal of Applied Business Research, Volume 21, Number 2
Wells II, Linton; Hailes, Theodore C. and Davies, Michael C. (Ed.) (2013), Changing Mindsets to Transform Security: Leader Development for an Unpredictable and Complex World, Center for Technology and National Security Policy, Washington
Williams, Paul D. (Ed.) (2008), Security Studies / An Introduction, Routledge, London & New York