Assessment of stress sources and moderators among analysts in a cyber-attack simulation context

Stéphane Deline, Laurent Guillet, Clément Guérin, & Philippe Rauffet
University of South Brittany
France

Abstract

With the prominence of cybersecurity questions, the role of analysts in managing cyber-attacks is crucial. Studies investigating human factors in cyber defence context generally focus on analyst training, situation awareness or cognitive biases (e.g. Gutzwiller et al., 2015) in order to reduce analyst errors. Champion and collaborators (2012) showed that social factors such as team communication influence the cyber teamwork. In this present study, we have examined elements contributing to the analyst's stress level. More precisely, we have studied the effects of cyber threats and the moderator effects of social support on analyst stress. We venture the hypothesis that 1) cyber-threats have an impact on stress levels and 2) social support reduce individual stress levels. This study has taken place in a cyber-security centre where cyber-attacks on a Vital Organisation have been simulated with engineer-students as cyber-defenders. Stress levels have been measured according to their heart frequency, and social communications have been coded from the video. Results show that threats do not directly affect stress, whereas obtaining -informational - social support is associated with a decrease of stress level.

Introduction

Many organisations (industrial firms, financial institutions, public administrations, companies operating in the fields of defence and energy or more generally organisations depending on the use of computer data or internet) have a critical need to protect against cyber-attacks. In order to ensure the security of their information system, these organisations need to get protecting against data theft and alteration. With the increasing number of cyber-crimes, it is essential to identify factors improving effectiveness and efficiency of cyber defenders. These operators have to assess how serious the situation is swiftly, identify priorities and make relevant decisions. The strong pressure (time pressure, high risk) felt by these operators can generate significant stress and therefore impact their performances. In this context, we will observe how the cyber team operates and is managed during cyber-attacks.

The aim of this exploratory study is to examine the effects of cyber events and the moderator effects of social support on stress level in cyber-attack simulation. This study takes place in a cyber-security centre where cyber-attacks on a Vital Organisation have been simulated with engineer-students as cyber-defenders.

In D. de Waard, F. Di Nocera, D. Coelho, J. Edworthy, K. Brookhuis, F. Ferlazzo, T. Franke, and A. Toffetti (Eds.) (2018). Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2017 Annual Conference. ISSN 2333-4959 (online). Available from http://hfes-europe.org

Theoretical framework

In the literature, Champion, Rajivan, Cooke, & Jariwala (2012) suggest that a cybersecurity analyst team can be characterized as a group of individuals working independently with few communication or collaborative efforts among team members. They identified three major factors impacting teamwork: overall organisation of the team, team communication and information overload. Some authors (Gutzwiller, Fugate, Sawyer, & Hancock, 2015; Champion & al., 2012) focused on situation awareness in cyber defence context but not on stress processes.

With regard to stress, several models exist. This study uses the Lazarus (1984, 1999) transactional model of stress. Stress occurs when person/environment transactions lead the individual to perceive a discrepancy between the situational demands and her/his resources or abilities to cope with those demands. The nature and type of coping generated by a person will be determined by the coping resources in the personal environment. The model identifies four types of coping resources: individual resources, social support, beliefs, and problem solving skills. Granåsen & Anderson (2015) explore the within-team communication in a cyber-attack situation to understand and get knowledge on team effectiveness in cyber defence exercises without taking social support into account. Our study aims to assess the relationship of social support on stress level. The social support will be measured through the communications. We focus on social support which is considered as a major moderator. Indeed, Kaufmann & Beehr (1986) suggest that positive communications might buffer individual occupational stress, while negative communications might have a reverse buffering effect.

According to House (1981), social support is defined as a positive resource that a person can use to cope with stressful situation. House (1981) distinguished four types of social support:

- Emotional support consists in expressing to a person the positive affect that one feels towards her (friendship, love, comfort, sympathy), and generating feelings of reassurance, protection or comfort.
- Appreciation support is about reassuring a person in terms of skills and values. This encouragement will allow her to strengthen her self-confidence in times of doubt when she is concerned that the demands of a situation will exceed her resources and capacities (overwork, role conflict, burnout ...).
- Informative support involves advice, suggestions, knowledge about a problem, proposals for solving a new problem, for example.
- Instrumental support involves effective assistance such as lending or giving of money or tangible goods or providing services in difficult times. It also characterizes assistance in the form of donating time or work.

Frese (1999) shows that social support buffers the effect of stressors on health. Buffer effects in the relationships between stressors and psychological or psychosomatic dysfunctioning are higher when social support is high and lower when social support is low. Malviya, Fink, Sego, & Endicott-Popovsky (2011) aim to determine whether situational awareness of team members participating in a cyber-competition could predict the overall team’s score. Various data were collected (e-mail, machine logs, video and audio sources), and they suggest supplementary data sources such as physiological stress measurements should be introduced in order to complete their research. The stress can be measured with heart frequency in dynamic situation (e.g. in driving, Healey & Picard, 2005). To our knowledge, no studies have been conducted on the assessment of stress in cyber defence situations, and none involves the study of heart frequency.

The objective of this research is to explore the effects of cyber events and the moderator effects of social support on analyst stress. We venture the hypothesis that (H1) cyber-threat have an impact on stress levels, and that (H2) social support reduces individual stress levels. We have designed a methodology to record all communications during a simulated cyber defence exercise, focusing on social support communications. The different situations of cyber-threats are then studied with regard to the potential stress generated. This stress is measured through heart rate and matched with social support.

Method

The cyber context

The study was carried out in the Cyber Security Centre (CSC) of a Higher National Engineering School in France. Cyber-attacks on a VO (Vital Organisation, e.g. an energy company) information system can be simulated. In order to be more realistic, a scenario of a hospital attack is worked out: following a series of triggering events (planned by the author's scenario), the repercussions of these events on the hospital and its environment were simulated (e.g., social conflicts) associated with a series of cyberattacks (e.g. DDOS, Defacement). These attacks could occur at any time during the day. The operators had no information on the development of the scenario and they had to resolve the situation using their defence skills. Several cells were constituted for the exercise management. The Cyber cell, called the Blue Team, constitutes the SOC (Security Operational Centre) in charge of the organisational security. There is a Management Team making choices and confirming the decisions, the Red Team launching the cyber-attacks, an Animation Team regulating depending on the sequence of events and a White Cell for interacting with the media and providing potential reinforcement.

Participants

The sample is composed of 29 graduate students from the engineering school of the University of Southern Brittany in France. They are aged from 21 years to 32 years (mean age = 23.,93 years, standard deviation = 2.62). The sample is composed of 1 female student and 28 male students. The participants' anonymity is guaranteed and a request for consent was signed by the participants fifteen days before the experiments.

Data collection

Observations and measurements of activity were made during an exercise of cyber defence simulation training. The Cyber Crisis Exercise took place over five days in

February 2017. Spread out in four teams, each team was placed alternately in the Cyber Security Centre in a cyber-crisis situation. In this study, the team focussed on is the Blue Team. It consisted in 6 operators and a Real-Time Coordinator (CTR) responsible for coordinating crisis management operations. They had to deal with threats and attacks that could damage the system of the simulated VO. A measurement of the heart rate (HR) of the team members was performed using a BioHarness3 ™ heart rate monitor, three days before the exercise for HR baseline calibration, and continuously, throughout each exercise day for physiological stress measure. Two cameras recorded participants continuously during the cyber-crisis exercise. Communication were recorded using microphones and dictaphones all along. All events, communication and activities (e.g. movements) were coded according to a coding scheme. The coding scheme was designed to identify cyber events and social support verbalisation.

The coding procedure was focused on taking the oral communications of the Blue Team into account. The coding scheme on social support was carried out in four steps: 1) Identification Sender (CTR or operator); 2) Purpose of social support (contribution, expectation or proposal); 3) Identification of the recipient (CTR or operator); 4) Qualification of the type of support (instrumental, informational, emotional, appreciation). For example, in the case of a social support contribution (SSC) from the CTR, SSC could take one of the four types of support cited above.

Proposition, expectation and contribution social support behaviours had been coded but for the illustration, the focus was on contribution. An example of each kind of contribution is presented in Table 1.

Table 1. Illustration of types of social support contribution (SSC) during the cyber exercise.

CONTEXT DESCRIPTION	COMMUNICATION (Op = Operator / CTR = Coordinator in real-time)	SOCIAL SUPPORT CONTRIBUTION TYPES
Op1 uses a tool that he doesn’t know very well and asks Op2 what he should do.	Op1 "What should I do in the software **Op2 "you click here** (showing directly with the mouse of the Op1’s PC)".	Instrumental
Op1 doesn’t know how to do an analysis task. Op2 responds.	**Op2 "For the UFW you do a ‘Ptinstall’, you look for the configurations Apt in each machine.**	Informational
The CTR has made a request for reinforcement. The reinforcement arrives. Here is the reaction of the CTR when he understands who the reinforcement is.	**CTR "Oh that’s a great gift"** [to have this person]	Emotional
CTR follows an Op task and encourages him in his task.	CTR "how is it going?" Op1 "I have made back-ups on my PC, in case the machine gets attacked." **CTR "It's good okay".**	Appreciation

Heart rate analysis and Controlled variables

In the analysis of heart rate (HR) variations, we decided to ignore a behaviour interval of 20s around the behaviour in order to exclude from the data, HR variation caused by the communications induced by the behaviour. When a studied behaviour occurred, we compared mean HR during 20s before (Interval 1) and 20s after the SSC behaviour interval (Interval 2) (see Figure 1).

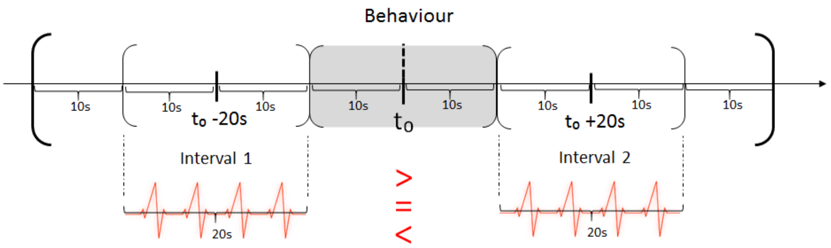

Figure 1. Heart rate comparison method.

Physical activity (standing or sitting position) was controlled around interval 1 & 2 to limit ecological context bias. The HR is known to be sensitive and slowly decreasing, so we controlled the activity of the individual in order to limit activity influence on HR. If the operator was not seated during a fixed interval (40 seconds before and after a studied behaviour), the behaviour was excluded from the analysis.

Results

The result section presents the effects of threatening cyber events on individuals and the effects of social support on individuals HR.

Threatening cyber events

In this part, the communications on threatening cyber events that contribute to collective representation among the cyber team is analysed. These events are: detection of threats, detection of attacks, or more generally additional information contributions on such events. It was found that 66 occurrences of these threatening cyber events were coded. After activity control (standing versus sitting position), only 30 occurrences of threatening cyber events were taken into account. The boxplot depicted in Figure 2 shows the variation of HR during these occurrences.

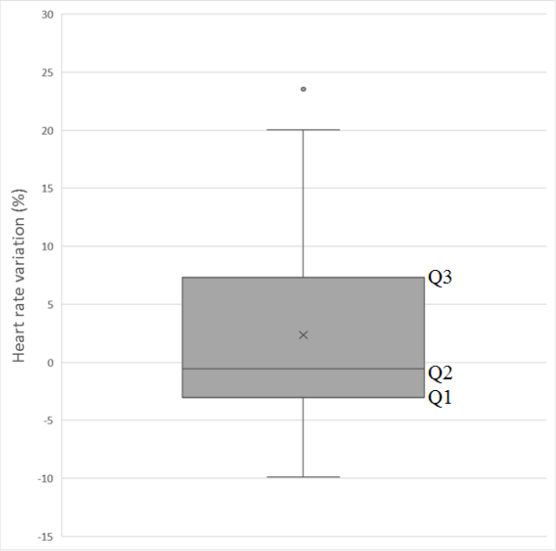

Figure 2. Variation of heart rate with threatening cyber events. Q1 = Quartile 1, Q2 = Median, Q3 = Quartile 3, × = Mean.

When comparing before and after the onset of threatening cyber events, no effect was found on HR (Mean = + 2.34 %; NS with a Wilcoxon paired test, n = 30). To illustrate, Figure 2 presents each individual HR pattern variation between interval 1 & 2 (see), depending on the criticality level of the cyber-attack (level 1: low hazard & low recovery, level 2: medium hazard & medium recovery, level 3: high hazard & high recovery; from a cyber-subject matter expert) in the simulation context.

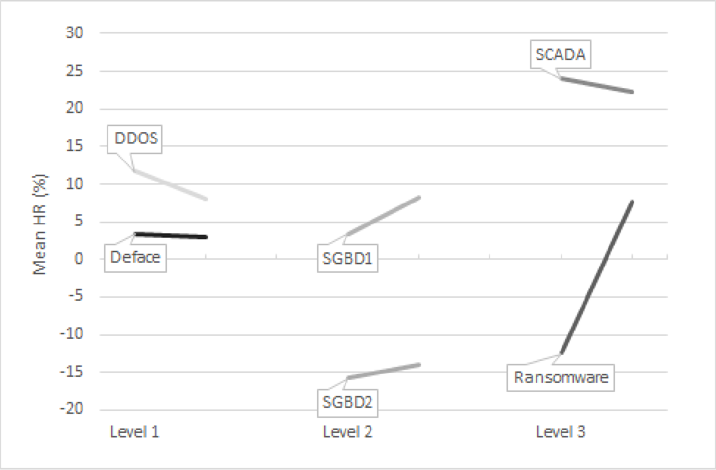

Figure 3. Heart rate variations depending on the criticality level of cyber-attacks (level 1 to level 3; n = 6).

The different individual patterns observed (Figure 3) suggested that attack criticality influences the individual reaction. When the attack criticality level was low (level 1), the 2 individual patterns did not indicate an increase of HR. However, when the attack criticality was higher (Level 2 or 3), pattern show an increase of HR except for the SCADA attack. An explanation of the decrease of HR for SCADA attack is that the individual already had a high HR before the attack, and so an increase of HR was less likely.

Social support

In this part, the social support behaviours were investigated. In total, 320 occurrences of social support behaviours were coded from communication. The most prevalent social support behaviours coded were contributions (n = 211) then expectations (n = 89) and finally social support propositions (n = 20). Among the social support contributions (SSC), the most frequent SSC was informational social support contribution (n = 144), then instrumental (n = 32), appreciation (n = 20) and finally emotional (n = 15).

In the following, we focused on the SSC, and analysed the variation of HR with its occurrences. In accordance with our second hypothesis, the analysis indicated a decrease of HR following a SSC (Mean = -3.410 %; W = 4.367; $p < 0.001$, with a Wilcoxon paired test, n = 117) compared to before the SSC.

In the boxplot depicted in Figure 4, the HR variation depending on SSC types are presented.

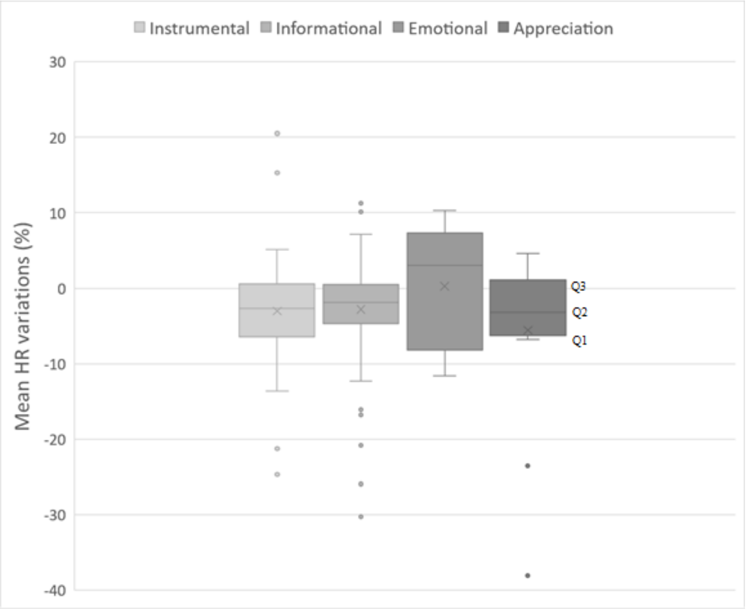

Figure 4. HR variations depending on types of social support contribution; Q1 = Quartile 1, Q2 = Median, Q3 = Quartile 3, × = Mean.

We differentiated SSC depending on the central tendency and the homogeneity of HR variations after these SSC. All SSC -except emotional- were associated with a HR median variation from -1 to -5% and an interquartile interval from 1 to -6 %. These distributions indicated that HR was stable or decreased for 75 % of SSC occurrences. The analysis of HR following a SSC showed a significant difference for informational SSC (mean = -2.886 %; t = 3.634, p < 0.003, n = 78) but not for instrumental SSC (Mean = -3.146 %; NS; n = 19), emotional SSC (Mean = 0.250 %; NS; n = 5) and appreciation SSC (Mean = -5.583 %; W = 2.166; p < 0.07; n = 15). These results are in accordance with our hypothesis of an effect of SSC on HR, depending on the type of SSC.

Discussion

The current study was conducted to investigate stressors (cyber-threats or cyber-attacks) and stress moderators in cyber context.

Cyber stressors

Our hypothesis that threatening cyber events increase stress among cyber operators is not verified. As Figure 3 suggests, the increase tendency of stress with cyber-attacks seems to be influenced by individual features and potential level of criticality of cyber events. First, as the Lazarus stress model (1984, 1999) proposes, it can depend on the individual personality which can be identified with appropriate questionnaires. Operators can be differently affected depending on their anxiety or current stress level. On one hand, if they are not anxious or engaged in their task, their stress level will be more stable. On the other hand, if they are already stressed, an increase of stress level is less likely. Such questionnaires have been administered and constitute the next phase of our research. Secondly, the specificity of the context which is ecological but not a real one, could affect their stress level. The fact that the exercise is a simulation can reduce impact of attacks compared to real live attacks, even if the exercise was also an evaluation of individual cyber defence abilities. Thirdly, the operators are trained to defend information systems from attacks, and with expertise, they have to manage stress during cyber events. So probably, threatening events are not the most important stressor, other factors, as validating countermeasure or making management decisions (e.g. to disconnect website) could be more stressful and constitute an interesting perspective for study.

Heart rate variation with social support contribution

In a general manner, social support contribution is associated with a decrease of HR. It provides an additional argument to the Lazarus model of stress (1984, 1999) that SSC is a relevant moderator of stress. It is also in accordance with the hypothesis of positive or negative communication buffering effect (Kaufmann & Beehr, 1986) suggesting that positive communication might buffer individual occupational stress. However, social support's contribution has different effects on stress depending on social support contribution types. Informational social support contribution reduces stress whereas the other types do not. More surprising is that instrumental social support contribution does not influence heart rate despite its tangible feature. One explanation is that a relevant tangible social support contribution can be very useful for the operator’s task, inducing new cognitive tasks and so potentially additional mental workload. It could be interesting to insert a combination of measures to control the impact of mental workload on heart rate. Moreover, appreciation social support contribution tendentially reduces heart rate which means that when an operator is stressed, discouraged or submerged, encouraging him could have a positive effect on stress. Under stressful conditions like a cyber-crisis context, encouraging or helping collaborators in need, could have an important effect on stress and so contribute to team cohesion. In a performance perspective, such a vector of team cohesion and stress could be an interesting way to optimize team functioning.

Conclusion

The study shows that in a cyber-attack context, threatening events may not be sources of stress but the attack criticality could be. Moreover, the social support contribution -and more specifically informational contribution- seems to moderate the stress level. It would be interesting to continue the investigation on stressors and moderators in a cyber defence context with a combination of stress and mental workload tools, in order to dissociate their respective influence on heart rate.

Acknowledgments

Thanks to the Cyber Centre of Excellence, the Brittany region and the University of South Brittany.

References

Champion, M.A., Rajivan, P., Cooke, N.J., & Jariwala, S. (2012, March). Team-based cyber defense analysis. *In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 2012 IEEE International Multi-Disciplinary Conference (pp. 218-221).

Frese, M. (1999). Social Support as a Moderator of the Relationship Between Work stressors and Psychological Dysfunctioning: A Longitudinal Study With Objective Measures. *Journal of occupational health psychology*, *4*, 179-192.

Granåsen, M. & Andersson D. (2015). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work*, *18*, 121-143.

Gutzwiller, R.S., Fugate, S., Sawyer,B.D., Hancock. P.A. (2015). The Human Factors of Cyber Network Defense. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59, 1, 322-326.

Healey, J.A. & Picard, R.W. (2005). Detecting Stress During Real-World Driving Tasks Using Physiological Sensors. in IEEE Transactions on Intelligent Transportation Systems, vol 6, 2, 156-165.

House, J.S. (1981). *Work and stress and social support*. Reading, Mass: Addison-Wesley.

Kaufmann, G.M., & Beehr, T.A. (1986). Interactions between job stressors and social support: Some counterintuitive results. *Journal of Applied Psychology*, *71*, 522-526.

Lazarus, R.S., Folkman, S. (1984). Stress, appraisal, and coping. New York, Springer Publishing Company.

Lazarus, R. S. (1999). Stress and emotion: a new synthesis. New York, US: Springer Publishing Co.

Malviya, A., Fink, G.A., Sego, L., & Endicott-Popovsky, B. (2011). Situational Awareness as a Measure of Performance in Cyber Security Collaborative Work. Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011. 937-942