МЕЃУНАРОДЕН ГОДИШНИК

НА ФАКУЛТЕТОТ ЗА БЕЗБЕДНОСТ

2024/1

INTERNATIONAL YEARBOOK

FACULTY OF SECURITY

2024/1

Publisher: Faculty of Security – Skopje

For the Publisher:
Dr. Sc. Jonce Ivanovski, Dean

ISSN 1857-6508 **DOI: 10.20544/IYFS.44.1.24**

CONTENT:

Editorial Notes

The scientific and professional papers that we publish in the duel of the International Yearbook of the Faculty of Security - Skopje, where the authors present their scientific and professional analyzes and findings from several scientific fields through their papers, namely: criminology , criminological, criminal-legal, police and other scientific fields that have their connection with security sciences and make a certain contribution to the development of scientific thought and a unique contribution to the development of criminal and police practice, which is of exceptional importance for practitioners and the application of science in practice with the aim of more successful performance of police and criminal activity in solving the complex problems we face in this dynamic time of new and serious security challenges.

I express my gratitude to the authors from the Faculty of Security in Skopje, fellow professors and doctoral students of our faculty, but also to the authors from other faculties at the University "St. Kliment Ohridski" - Bitola, authors from other Universities who, through their papers, bring us their theoretical studies and research results from the respective fields related to security and dealing with security challenges.

In the double issue of the International Yearbook for 2024, 10 papers are published, which cover topics from several security areas, which I hope will provoke your attention to read, analyze and apply accordingly in your scientific studies and research in part from their research results and theoretical analyzes of the respective problems.

I express my pleasure that with the publication of the double issue of the International Yearbook continuously since 2005. the renewed tradition of publishing this international scientific journal at the Faculty of Security in Skopje is continuing.

Sincerely,

Editor of the International Yearbook of the Faculty of security

Professor Bogdancho Gogov

UDK: 364.622:351.74.082(497.7)

MENTAL HEALTH CARE OF POLICE OFFICERS IN THE REPUBLIC OF NORTH MACEDONIA

Dragana Batic
Faculty of Security – Skopje,
University St. Kliment Ohridski Bitola, North Macedonia
dragana.batic@uklo.edu.mk

Abstract

The purpose of this paper is to point out the importance of police officers' mental health through a series of studies in the world, where the issue of the impact of stress on the individuals in police organizations has not only been researched for years, but the results of the studies are applied in practice, so they are actively working on raising the resilience of police officers through specific programmes for psychosocial support.

The paper deals with the treatment of stress and mental health of police officers in the Republic of North Macedonia, through the presentation of two empirical studies: one refers to the state and psychosocial reactions to stress from the war among members of the security forces, participants in the 2001 conflict, and the second is about the stress reactions of police officers during the Coronavirus epidemic. The results of the two surveys show that, in the Republic of North Macedonia, no account is taken of the surviving stress of the members of the police and its impact on mental health. Recommendations are given for improving the care of the police officers' mental health in general, and especially after stressful events within the performance of professional tasks.

Introduction

The police profession is one of the most stressful professions because police officers are exposed to potentially high-risk situations during their work, such as the risk of injury and murder. Additionally, there are other significant factors, such as suppression of emotions, self-medication, toxic work environment, unsupportive organization, lack of support from colleagues, the image of the police in the media which tends to portray them as bad, corrupt and brutal, rather than professionals who do their job honestly. On the other hand, public expectations of the police officer, who should be someone who is invincible, creates an image of a superman, someone who must not show weakness, which leads to the stigmatization of those with mental disorders and to self-stigmatization that leads to resistance to seeking psychological help and support. All these circumstances and expectations are intertwined and create negative consequences for police officers' mental health. Failure to identify and address issues related to it can have consequences for police officers and their families, such as depression, divorce, illness and even suicide.

"Research shows that this category of employees suffers negative consequences that include burnout (Asmundson & Stapleton, 2008), sleep problems (Fekedulegn et al., 2016), cardiovascular disease (Violanti et al., 2013), post-traumatic stress disorder (Martin et al., 2009), neurological disorders (Covey et al., 2013), addiction diseases (Benedek et al., 2007),

depression (Hartley et al., 2007) as well as death caused by suicide (Violanti, 2004) (according to Papazoglou, 2021).

Risk factors for police officers' mental health

Physical, physiological and emotional stressors in police work fall into three categories: extra-organisational, intra-organisational and individual (Lawrence, R.A. 1984). Extra-organizational are those events that cause stress but are outside the police organization; intra-organizational originate from the police organization; and individual refer to the personality characteristics of the police officer.

Unlike people in other professions, police officers begin their careers exceptionally healthy and, over the course of their working lives, develop a wide variety of stress-related disorders. Stressful life events include explosive, implosive and corrosive incidents (Waters, J., Ussery, W., 2007).

Explosive events are some serious criminal or terrorist situations, military conflicts and natural disasters that lead to acutely difficult emotional reactions in the police officer, which he/she usually suppresses in order to continue fulfilling his/her role as a protector of citizens. Long-term consequences occur when interventions that would help mitigate and overcome them are absent.

Some events have an implosive nature due to an internal conflict, that is, a value system that guides a person in choosing a profession. The most common conflict, between family and personal responsibility, on the one hand, and professional responsibility on the other, continuously lead to the development of stress symptoms.

Everyday tensions have a corrosive effect, because there is a decrease in confidence and a decrease in resilience and flexibility of the person. Night shifts and overtime work interfere with a normal family life. Changing the rhythm of sleep affects physical and mental well-being. An essential problem, especially with corrosive events, is that the individual ignores them and does not engage to protect himself and his well-being (he ignores personal difficulties, does not seek medical and psychological help, does not cultivate healthy lifestyle habits, uses unhealthy coping mechanisms etc.). The police organization also ignores the negative consequences of police work (Waters, J., Ussery, W, 2007).

A factor that negatively affects police officers' mental health is the police culture, which emphasizes emotional control and masculinity in police work (Edvards, Kotera, 2020). As a result, one is expected to suppress emotions in front of others and show firmness (Porter, Lee, 2023).

Resorting to dysfunctional ways of dealing with stress, as a common pattern among police officers, includes consumption of alcohol, which is used for relaxation, is socially acceptable and contributes to a macho image. Although it contributes to a temporary reduction in feelings of depression and inhibition, in the long run, it leads to more problems, such as marital problems, road accidents and physical ailments, and even to suicide or murder.

In this regard, the question arises as to how to prevent dysfunctional behaviour of police officers. One of the ways is certainly psychotherapy. However, most police officers avoid seeking help because they distrust psychologists and psychiatrists, due to the stigma attached to mental health problems that stems from a police culture where mental health problems are considered a sign of weakness. In this contect we can also include ignoring symptoms of depression such as decreased energy, feelings of sadness or worry, fear of losing their job if they seek help (Hackett, D.P. and Violanti, J.M., 2003). Defence mechanism such as negation (denying the possibility that they can be hurt), not having a

backup plan for the future for themselves and their family also makes them sensitive. Police officers are "too proud and too timid" to seek help for themselves and their families (Kirschman, E., 2000).

Although research has not shown that there is a single psychological profile of a police officer, there is a consensus that the police profession generates certain behavioural characteristics. For example, a police officer can become suspicious, rigid, cynical and authoritarian. Dealing with people who are criminals and hostile, leads to mistrust that over time they begin to manifest towards their friends and even their family members (Hackett, D.P. and Violanti, J.M. 2003).

One of the biggest risks of police work is narcissism, self-centeredness. They invest most of their time in their work, so they become untrustworthy and unsupportive, and thus alienate themselves from their family. (Waters, J., Finn E.,1995). Kirshman points out that the domestic violence that occurs in the families of police officers is "police's best-kept secret... The presence of guns and the ability to use them makes 'police officers the most dangerous group of domestic abusers and their wives the most at risk'" (Kirschman, E., 2000).

All these risk factors should be taken into account in terms of overcoming them in order to improve police officers' mental health.

Mental health among police officers in the Republic of North Macedonia

As an illustration of the attitude towards police officers' mental health of the competent institutions in the Republic of North Macedonia, we will present the results of two empirical studies on the mental state of police officers that relate to two situations that have occurred in the last thirty years in Macedonia and include events in which strong stressors are present as a threat to police officers' mental health: one is the conflict from 2001, and the other is the Coronavirus pandemic in 2020.

Psycho-social consequences among members of the security forces from the 2001 conflict

In 2009, a survey was conducted on the psychosocial consequences of the security forces of the Republic of Macedonia, participants in the 2001 conflict, on a representative sample of 667 respondents, from among the members of the Ministry of Internal Affairs, the Army, the reserve forces and the village guards.

The following hypotheses have been tested:

1. The exposure to military stress during the 2001 conflict among the members of the security forces who participated in it leads to psychological, social and behavioural reactions;
2. Some members of the security forces experience psychological consequences in the form of PTSD symptoms, depression, anxiety and aggressiveness due to exposure to military trauma;
3. The severity and number of traumatic experiences affect the presence of symptoms (PTSD, depression, anxiety and aggression);
4. The presence of symptoms (PTSD, depression, anxiety and aggressiveness) that affects the family relationships of the members of the security forces and their families.

5. The presence of symptoms (PTSD, depression, anxiety and aggressiveness) affects the relations of members of the security forces at the workplace.

About the assessment of the psychological state of the participants in the 2001 conflict. the following psychological instruments were used:

1. Clinical anxiety scale (CAS), Bruce A. Thyer, 1986;
2. Beck Depression Inventory -BDI, (Beck, A.T., 1967);
3. Impact of Events Scale –IES (Horowitz, M. J., Wilner, N., and Alvarez, W. 1979);
4. State Trait Aggression Scale – STAS (Spielberg, C. D., Jacobs, G., Russel, S., and Crane, R.S., 1983).
5. Questionnaire for assessment of military stressors, which is a questionnaire taken from Serbia and adapted for our conditions (Questionnaire for assessment of war stressors, Jović, 2002). This questionnaire covers a wide range of stressors characteristic of the military conflict in the territory of the former Yugoslavia, to which, in addition to soldiers, civilians were also exposed.
6. A questionnaire on family relationships, constructed specifically for this research, contains questions related to: agreement with the wife/partner, the way of solving problems in the family, the way they evaluate their family according to its functionality, the presence of socio-pathological phenomena in the family, noticeable changes in relations with close people after the 2001 conflict.

The data has been processed statistically, in addition to descriptive statistics, several statistical methods have been used, primarily regression and factor analysis. [1]

Results

The results show that the respondents survived events with a high degree of stressogenicity, which represented a direct or potential danger of death, vulnerability or threat to personal or other people's physical integrity. As a result, psychological changes occurred in them, of which the most pronounced changes are in the sphere of emotional processes. Namely, the participants show increased anxietz, depression, aggression and symptoms of PTSD.[2]

According to these results, more than half of the defenders show symptoms of depression and anxiety, as well as symptoms of PTSD: involuntary imposition of trauma-related impressions and avoidance of anything reminiscent of the trauma. Aggressiveness is much higher, and more so when it comes to aggressive feelings and less aggressive reactions. This means that, although they have a feeling of anger, the subjects control themselves in terms of its manifestation. Or as one of the participants in the research said: “We are like a time bomb”. These results are in accordance with existing knowledge in the field of stress psychology (Card, 1987, Foy, 1987, Zotovic 1993, Novovic, 1994, Kulka, 2013, Vári, Vince 2023).

The presence of symptoms (PTSD, depression, anxiety and aggression) is related to the severity and number of traumatic experiences. Stressful events, characteristic of participation in war, such as combat actions and other experiences with which the defenders' lives or the lives of others were threatened, had the greatest influence on the occurrence of

[1] Ibid.
[2] Ibid.

stress reactions. Thus, the results of the applied regression analysis show that exposure to war stressors has highly significant multiple correlations with individual indicators of psychopathology that are usually considered psychological consequences of exposure to stressors: depression, anxiety, aggression, imposition and avoidance of thoughts related to the traumatic event.

The presence of symptoms indicating PTSD, as well as symptoms of anxiety and aggression, give an image of these persons as a high-risk category in terms of mental health in our society. From the factor analysis of the psychological variables, one significant main component was obtained, which could be interpreted as a general psychological factor, which we called the factor of traumatization.

The current symptoms of traumatization affect the respondents' relationships with other people, especially with those close to the family in terms of dysfunctional functioning: avoidance of closeness, tendency to conflicts, interruption of communication, leaving home and even psychological and physical violence. It is known that a traumatized person in the family acts as a factor of traumatization of the family system, as he finds it harder to cope in his role, frustrates others with his sensitivity and reduces communication with loved ones. Obviously, for our respondents, the experience of participating in the 2001 conflict led to consequences, which the competent state authorities did not take into account and did not offer them the opportunity for recovery and psychological healing.

"The results of this research show that exposure to stressful events during participation in the conflict, which were numerous and multiple, led to multiple stress reactions: anxiety, depression, PTSD symptoms (avoidance and intrusive thoughts) and aggression. These reactions, in turn, affected changing relationships with others, especially in the family in terms of increased presence of conflicts, aggressiveness and distancing from others."[3]

The traumatic experiences they experienced led to stress reactions, which after the end of the conflict persisted due to their non-resolution and due to insufficient support from society. The problem with trauma, in this case war trauma, is that it doesn't diminish over time, but it persists. Current life events, especially feelings of rejection, alienation and misunderstanding from the environment interact with the existing symptoms of traumatization that lead to maintaining and complicating the said emotional state.

The research, the results of which we presented, was conducted eight years after surviving the participation in the military conflict. Experiencing a traumatic situation requires the fastest possible intervention, that is, intervention in a crisis. Since she was absent, even after a long period of time, the symptoms continued to persist.

The obtained results indicate a serious psycho-social situation of these persons. While the professionals of the countries in our environment (Croatia, Serbia, Bosnia) at the time when the research was conducted, were worried because in their circles there is a lot of talk about this problem, and very few concrete actions are taken to help the war veterans, in our country the mental condition of the participants from the conflict was not even discussed at all.

Among military veterans, over time, as our research shows, traumatization does not decrease, rather, it increases. Such a condition affects difficulties in solving everyday life problems in a constructive and adequate way; there is a withdrawal from social life and an

[3] https://fb.uklo.edu.mk/wp-content/uploads/sites/10/2021/12/ISTRAZHUVACHKI-IZVESHTAJ-ZA-PSIHO-SOTSIJALNITE-POSLEDITSI-OD-2001-GODINA.pdf.

accumulation of dissatisfaction, anger, guilt, and as a consequence: divorces, problems at work, domestic violence, addiction problems, and even suicide and murder attempts can occur. Thus, being traumatized affects an intrapsychic and intrapersonal plan, which leads to complications primarily in family relationships, but also in relationships with others in general. In this way, the family members also become traumatized, so that this problem is transmitted transgenerationally to the children. The end result is the social isolation of these persons.

At the time of the research, the authorities did not recognize the problem, which could be seen by the absence of psychological help and support from the police. And after the publication and public presentation of the results of the research, where we advocated to change it with a series of proposals, such as the introduction of psycho-social support to overcome the consequences that are still current, through the opening of regional counseling centers in Macedonia, individual psychotherapy, group psycho-social intervention in order for the groups to grow into self-help groups. None of it was accepted. Unfortunately, this situation did not change, even later, in other cases, when police officers were exposed to stressful events such as endangering their own lives and the lives of their colleagues (for example in the case of "Divo Naselje 2015").

Psycho-social (non) support during the COVID pandemic

This research is part of the combined interdisciplinary project of the Faculty of Security under the title "The functioning of the security system of the Republic of North Macedonia in conditions of emergency and crisis – case study", and deals with the psychosocial aspect of the crisis.

In 2020, the emergence of the global infectious epidemic with SARS-CoV2, a dangerous and still unknown virus, led to numerous changes in the life of the population such as the threat of infection, fear and uncertainty and the measures of self-isolation, social distance, restriction of movement, learning from home, working from home and losing a job, which negatively affected metal health.

This part of the research had two objectives: one was to assess the frequency of psychological issues and the level of resilience of health workers and police/army personnel, who during the pandemic were on the front line in the fight against this disease, compared with the results of the general population. For this purpose, an anonymous online questionnaire was prepared consisting of several self-assessment scales that measure: anxiety, depression and PTSD symptoms, as well as the degree of resilience. The following psychological instruments were used in the research: Scale for generalized anxiety disorder - Generalized Anxiety Disorder Scale-7 (GAD-7) Short Post-Traumatic Stress Disorder (PTSD); Rating Interview (SPRINT-8) ; Patient Health Questionnaire-9; Connor-Davidson Resilience Scale (CD-RISC-10).

In addition to these scales, the questionnaire contained demographic and other characteristics of the respondents as well as the way they deal with stressful situations privately and professionally.

The second goal of the research was the readiness of the state to react in crisis and emergency situations, in terms of mental health, i.e. what is the social response to the crisis in the area of psychosocial support of the population, risk groups and professionals, i.e. is there a system of psychosocial support in crises and emergencies?

In this part of the research, the following methods were used: observation and semi-structured interview, with: professionals who were and are in quarantine (police officers,

doctors and other persons), the managers of governmental and non-governmental institutions and their communication, as well as senior government officials (the President and the Prime Minister). The Covid-19 pandemic, restrictive measures, social isolation, the fear of getting infected personally and their loved ones, the increased workload are some of the factors that negatively affect the mental health of healthcare workers. The police officers who were involved in the research were at constant risk of becoming infected and passing the disease on to those close to them, which was a continuous and added stress to the whole situation. The survey showed that medical workers, as expected, felt the most threatened. Although the police and army forces coped with the situation with less deterioration of their mental health, perhaps due to previous training in dealing with stressful and violent situations, the results indicate that again, and in this case psycho-social support in the police organization, as well as for the medical workers is absent.

"Our organizations (health, the Ministry of Interior, fire stations) unfortunately lose sight of the fact that people who are professionals are vulnerable human beings with common reactions to stress, and that they need support to protect their mental health. Working with people who are under stress, whose lives are at risk, is an integral part of their work and is a complex process.... The responsibility for the mental health of its employees in general, and especially in conditions of crisis and emergency, which places greater demands on them than usual, certainly lies with the organization in which they work... it must prepare them psychologically for the stressful events for which it is known that they will face and during the crisis to offer them psychosocial support... in order to prevent the deterioration of the mental state of employees, to mitigate and reduce long-term psychological, social and physical consequences and to speed up recovery" (Batic et al., 2020).

The unwillingness of the organizations in general, including the Ministry of Internal Affairs, to deal with the mental health issues of their employees during the Covid pandemic has come to full expression. One of the recommendations from the research was to establish a system of psychosocial help and support that will prepare employees before a crisis occurs and provide them with psychosocial support during the crisis and after the crisis.

Mental health prevention in the police environment

In Great Britain, the stress presence in police officers and their managers is estimated to be 25% of working time, to increase awareness of the causes of stress and its reduction (Hirsh, R. M, 1999).

The FBI has developed the CISM (Critical Incident Stress Management) programme, for the protection and development of psychological fitness after traumatic events, such as burglaries, hostage situations, loss of a colleague in action and similar events. After such events, it is important to get psychological help and support several hours after the incident, in the form of a conversation. After a few days, a group discussion is applied, then group meetings with those who have had similar experiences, so that finally the family and manager of the person are involved. (Hirsch, 1999). It is believed that this method of intervention can be effective in other countries as well.

From the countries in our region, in Slovenia, there is an anti-stress programme intended for police officers, which has been in place since 1998. His evaluation showed that police officers are satisfied with the content of the programme and that it helps them in their daily work (Visnikar, Hedviko, and G. Mesko, 2002).

In the Republic of North Macedonia, unfortunately, there are no preventive programmes. The exception is that in 2002, the Police Union organized a week-long

preventive programme for policemen wounded in the 2001 conflict, in which the author of the test was one of the hosts of the programme. It is the only such programme at the state level.

The author of this test, on several occasions and through research and during official meetings with the members of the police leadership, has offered a programme for sensitization and dealing with stress as a preventive programme, which has not been implemented to date.

Conclusion

Police officers are exposed to stress during their work. Stressors can range from cumulative (constant job risk, police culture, public opinion, relationships within the police organization itself to incidents such as exposure to violent crime, shootings, stress during mass accidents, and participation in armed conflict as the strongest stressful situation that can last longer). Stress reactions, if left untreated, can lead to serious physical and mental health consequences.

The presented research shows that both in 2001 and 2020 the Ministry of the Interior, which is responsible for police officers, takes care of their mental health, even in highly stressful situations that are assumed to have a negative impact on the same.

To prevent these consequences, programmes are recommended for recognizing the symptoms of stress, for managing emotions that occur during stressful situations. In this way, police officers will receive a tool that will help them overcome stress in personal and professional situations. The leadership in the police must play an active role, that is, provide a sufficient number of psychologists and other professionals who will enable their employees to do so.

UDK: 351.74-051:316.46.058

LEADING POLICE IN A COMPLEX WORLD THE LAWS MODEL TO UPLIFT LEADERSHIP CAPABILITY

Tracey Harris
PhD Candidate, Griffith University, CEO Amovita International
Alex Caruana
President, Australian Federal Police Association
Trpe Stojanovski
Professor, External Associate, Faculty of Security, St. Kliment Ohridski University, North Macedonia
Elyse Leonard
Operations & Business Advisor, Amovita International

Introduction

Policing is a challenging and demanding profession, complicated by societal and individual expectations, and unique because of the contextual environment in which this profession operates. Overexposure to trauma and stress continually erodes emotional resilience, reducing law enforcement officer's ability to perform the intricacies of the role (Simmons-Beauchamp & Sharpe, 2022). Further, it places these professionals at risk as citizens often see the police as the keepers of safety in their communities. Given these demands, policing has dramatically changed with divergent terrorist threats, technology and new types of crime (Filstad et al., 2020).

Additionally, COVID-19 has shown that policing is affected by another angle, the global pandemic threats, which impacted the performances of the police organization and the health of the police officers as they were regarded as essential workers to enforce law and order (Helfers & Nhan, 2022). This has seen a rise in law enforcement officers encountering increasing levels of psychological stress, and frequently observing complex situations that can profoundly impact their mental health and quality of life. Due to far-reaching global societal challenges, the police are frequently exposed to life-threatening situations which increase the risk of elevated stress levels (Drew & Martin, 2023). Over time, if not addressed, the accumulation of stress increases the imminent probability of health issues and, if unresolved, can lead to serious and long-lasting problems.

In an international study between Australia and the United States (Drew & Martin, 2023) focused on wellbeing, 44% of the police reported they continually struggled with stress, depression or anxiety that was measured at a moderate to severe level. Participants reported the likelihood of future attempts to take their own life, and over 13% reported being suicidal throughout the previous year. Compared to the general population, the police face a 54% higher risk of this type of fatality. When asked where they seek support, they mainly talk to their spouse or colleagues, with only 22% likely to engage with other professional support or coaching services. Occupational stress related to shift work, negative societal perceptions and attending traumatic events, all resulted in mental health risk and reduced recovery from emotional injury (Simmons-Beauchamp & Sharpe, 2022). If left unmanaged,

diminished wellbeing and poor performance ensures a compromised workforce globally (Anderson et al., 2015).

The stigma associated with the language of mental illness often associated with prolonged stress, and lack of confidence in professional services to provide support, remains a barrier for many police officers accessing regular debriefing and a place to refuel through formal supervision with their police leaders. To address these complexities, risk reduction strategies require new thinking to enhance leadership capability and provide access to formal supervision that is regarded as a professional response to these challenges. This global crisis calls for urgent change to the way in which police leaders are trained and supported to use the latest evidence base in leadership and supervision, including the use of evidence-informed models (Harris, 2020).

Policing Leadership

To fully appreciate the importance of effective leadership, police culture needs mentioning. Culture is determined by all individuals through their identity based on values, and the power evidenced by the inter-connections between law enforcement officers, their leaders and the community (Beauchamp & Sharpe, 2022). Police culture has predominantly been cultivated by the uniform rank, for example, as a street cop vs top command leader (Filstad et al., 2020). In some police settings, police culture could be mapped separately between the uniformed police officers, as the most populated structure in the police, and the law enforcement persona, with specialized division of tasks and mindset. Both structures coexist in the organization, but also, they have internal differences, mostly presented in the ranks, the salary and the hierarchy.

Perceptions of leadership are further influenced by power located in the upper levels that dominate the narrative through status and rank (Davis, 2018). Often viewed as an environment that is led poorly, police culture has often created a setting in which the police do not reflect or discuss the impact of the complexity in their roles. Leaders set the standard influencing how values and connections are implemented and practiced. Assimilating police culture begins in recruitment programs and continues as cadets progress through the ranks. Indoctrination to the system is deemed to be complete when individual officers and leaders have fully adjusted to the norms which are, unfortunately, defined by organizational motivations and delegated authority (Beauchamp & Sharpe, 2022). Where law enforcement officers endeavour to break tradition from the normalized culture, they can feel isolated, burdened and compromised, resulting in wellbeing and performance impacts.

Police leaders are the key to breaking these sad realities and changing the discourse that continues to plague these perceptions, whether real or not. Therefore, the question needs to be asked about what constitutes effective leadership practice in policing and what assists leaders to shift their mindset and take leadership capability seriously. Filstad et al. (2020) suggest that leadership needs to expand leadership learning beyond context-dependent encounters that operate in a closed environment, given that individuals hold responsibility for how leadership practice is understood and practiced.

Leadership is often experienced as a bureaucratic process, focusing on accountability and maintaining control (Davies & Heysmand, 2021) in the policing environment. The directive context in which policing occurs, places leaders at the coalface of balancing managerialism and operative demands (Filstad et al., 2020) at the behest of

using leadership theories and approaches that demonstrate awareness of the elements that espouse focused leadership practices and the use of key frameworks (Harris, 2020).

Whilst leadership commonly encapsulates specific capabilities, for example, skills, attributes, tasks and knowledge (Harris, 2020), there is little evidence of how police leaders are both trained or required to demonstrate these through formal or informal evaluation processes. Therefore, at their best, leadership capability is often determined by the context of the role and how they perform through the eyes of higher-ranking roles (Carroll, 2016). The success and failures of the role are based on previous experience or from collegial modelling on the job, rather than from attending formal training, supervision or the use of leadership models (Harris, 2020).

Filstad et al. (2020) contend that police leaders need to comprehend what is required to demonstrate discrete capabilities that engage law-enforcement officers in meaningful discussions that promote high level practices, wellbeing and ongoing growth. Further, they suggest, the question remains as to how to make sure that the leaders develop ongoing leadership capability and evidence their ongoing effectiveness. Therefore, leaders must be socialized into new ways of thinking and learning through training programs, the use of models and engaging in their own supervision and coaching to evaluate their efficacy (Harris, 2020). Learning methods, including reflection and action-based experiential learning, dominated by tacit understanding, assist to transfer skills and knowledge in an authentic manner.

Globally, there is limited training focused on essential concepts related to leadership capability and the use of models that provide leaders with the skills and knowledge necessary for conducting effective conversations. There are also no known models in which police leaders can evaluate the effectiveness of their leadership based on their own self-report and or with their subordinates. Without a change in the way that leaders are trained to use these discrete capabilities, mental health issues will continue to plague law enforcement roles.

Filstad et al. (2020) found that, when police leaders attend quality training, it enables them to better understand what leadership practices make a difference, raises awareness about the range of capabilities required to be effective and validates their existing knowledge. It gives leaders confidence and the ability to move up the organizational structure with a higher level of capability and confidence in knowing they are effective. Attending training also offers the opportunity to reflect on oneself and understand key theories and practices necessary to master the role. Sharing the experience between the police organizations, nationally and internationally, especially when the mental health issues are in question, which is tabboo in various police organizations, is seen as very positive example for improving police knowledge and vision for more effective outcomes.

LAWS™ Leadership Model

Leadership models are visual representations that define how effective professional discussions occur. They aim to provide leaders and law enforcement officers with a comprehensive way of exploring all areas of the professional role using their leadership skills, knowledge, attributes and tasks (Harris, 2020). When applied consistently, they refine how discussions take place with purpose and intention, demonstrating how to focus the discussion

in these four areas. Given the model is illustrated in a well-defined diagram as illustrated in Figure 1, it assists both parties to set an effective agenda to better suit policing needs. The model is highlighted by quadrants that feature suggested agenda items that align to the professional aspects of the work, meet the requirements of the role, a mechanism for regular support and enhancement of knowledge and skills.

The LAWS™ model developed by Harris (2020) and endorsed by the Australian Federal Police Association to support police leaders in the law enforcement setting was recently presented at the International Police Executive Symposium. Harris (2020) has developed in excess of 30 models for leaders in different workplace contexts that support enhanced capability and ensure conversations with teams are focused and evidenced through the use of leadership theories and practices.

Illustrated in a circle equally divided into four areas for professional discussions, the model focuses the discussions on the *Law Enforcement/Professional* (L) aspect of the officer's role, including discussion items relating to ethical standards, decision making, feedback and maintaining professional and personal boundaries. The agenda may include a focus on developing and maintaining a professional identity and using a robust decision-making framework. When discussing aspects of the professional role, the leader uses a reflective style of communication to ensure that all professional aspects of the role are reflected in a productive way.

The *Administrative/Operational* (A) area of the model encourages discussions about the office meeting the requirements of the role. The agenda may include how tasks and processes are completed and ensure adherence to policy and procedures. This aspect of discussions explores maintaining accountability in the role and meeting organizational requirements. Leave requirements and workflow management are key aspects in this area of discussions and how workload is prioritized and scheduled. When discussing these agenda items, the leader adopts more of a directive style of communication to ensure key aspects of the role are met.

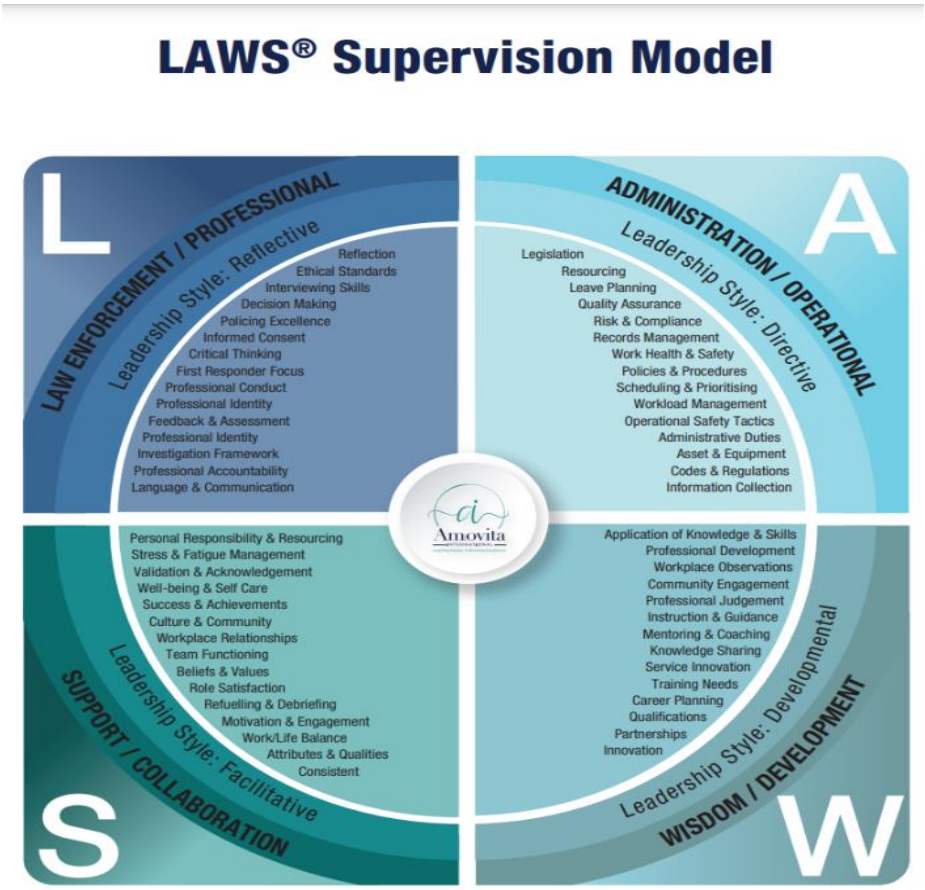
The *Wisdom/Development* (W) area of the model focuses discussions on ongoing growth and development of the law enforcement officer in the role. Training needs are discussed and the importance of ongoing professional development. Discussions may also focus on career planning and how skills are applied in the role using the transfer of knowledge. Leaders engage mentoring and coaching in this part of discussions and a focus on qualifications and learning development needs are also explored. When discussing these aspects of the role, the leader uses a developmental style of communication to ensure they maintain a focus on growth and development needs and address gaps in officer's capabilities.

The fourth aspects in discussions are depicted in the *Support/Collaboration* (S) quadrant of the model. Agenda items may focus on the reduction of officer's stress and fatigue, maintaining wellbeing and self-care. The discussion also includes role satisfaction and referral options to workplace support services. Other agenda items may focus on how to maintain motivation and engagement, maintaining professional workplace relationships and the importance of culture and community engagement. When discussing items in the S quadrant, leaders engage a facilitative style of communication to support officers to reach conclusions about their support needs.

Leaders can evaluate the focus of discussions and, over time, the model encourages leaders to be well focused and know what leadership skills and techniques to use to be highly effective (Harris, 2020). When using a range of capabilities that forecasts outcomes, leaders refine ways in which to have these professional conversations on a regular basis.

Both the leader and officer review the visual in meetings, which prompts both parties to consider what is a priority to discuss and empowers the officer to focus discussions on what is important for them to maintain performance and wellbeing in the role. Leaders then use key capabilities through their skills and knowledge to ensure conversations are dynamic and productive in meeting the officer's and organizational needs.

Figure 1. The LAWS™ Leadership Model



Conclusion

An evidence-based leadership model for law enforcement officers, such as the LAWS™ model, addresses the critical need for leadership training that ensures leaders understand what skills and knowledge are required for focused discussions using leadership models such as the one outlined in this paper. By focusing on key concepts that increase leadership development and effective communication techniques, the LAWS™ model equips leaders with the necessary focus to discuss and manage law enforcement officer's stress, foster mental wellbeing, and support their teams without taking on the burden themselves. Implementing such a model in police organizations ensures that leaders are better equipped to handle the psychological and emotional challenges inherent in law

enforcement and policing work, promoting a healthier and happier workforce. This approach not only improves individual wellbeing but also enhances overall performance and community trust. When leaders attend training and use a model such as this, their effectiveness in leadership increases exponentially. Emphasizing principles of neurocare and trauma responsive leadership through structured training and the use of the LAWS™ model provides the impetus for change and how we all work in partnership towards a world that helps police to reduce their stress and increase positive health outcomes, for we all need them to feel healthy, happy and well.

References

Anderson, J., Papazoglou, K., Arnetz, B., Collins, P. (2015). Mental preparedness as a pathway to police resilience and optimal functioning in the line of duty. *International Journal of Emergency Mental Health and Human Resilience 17*(3), 624-627. https://doi: 10.4172/1522-4821.1000243

Davies, A., & Heysmand, M. (2022). Implications of a field-based police leadership development programme. *Policing: A Journal of Policy and Practice 15*(2), 741-758, https://doi.org/10.1093/police/paz063

Davis, C. (2018). Rank matters: Police leadership and the authority of rank. *Policing and Society, 30*(1), 10-16. https://doi:10.1080/10439463.2018.1555250

Drew, J. M., & Martin, S. (2023). Mental health and wellness initiatives supporting United States law enforcement personnel: The current state-of-play. *Journal of Community Safety and Well-Being*, *8*(Suppl_1), S12-S22. https://doi.org/10.35502/jcswb.298

Filstad, C., Karp, T., & Glomseth, R. (2020). How police leaders learn to lead. *Policing 14*(3), 601-615. https://doi:10.1093/police/pay043

Harris, T. (2020). *Successful supervision and leadership*. Routledge.

Helfers, R., & Nhan, J. (2022). A qualitative study: An examination of police officers' lived experiences during the COVID-19 pandemic. *International Criminal Justice Review*, *32*(3). 308-327. https://doi:10.1166/10575677211050427

Simmons-Beauchamp, B., & Sharpe, H. (2022), The Moral Injury of Ineffective Police Leadership: A Perspective. Front Psychology, 13. https:// doi:10.3389/fpsyg.2022.766237

UDK: 351.746.5:316.654
316.774:351.746.5

THE ROLE OF THE MEDIA AND THE PUBLIC TRUST IN THE POLICE

Julija Popovska-Aleksandrovska L.L.M.
Senior Police Advisor
Ministry of Interior of the Republic of North Macedonia

Abstract

In an era of Internet, social networks, smartphones, underregulated media space on portals, and also political influences, it is hard to manage information affecting the Police and policing. Fake news often affects the confidence in the Police, hence the media can affect the Police reputation in the public, and also destructively act in the police environment itself, thus reducing work efficiency.

Various televisions create via portals such a picture of the Police by publishing news of crime and thus affecting the public perception of the state of society on security, whether citizens live in a safe society and a safe environment. The presentation of crime and police activities in the mass media are related to public perception of security risk and influence both the fear of crime and public trust in the police organization.

Public opinion comes as an ultimate result of the police work, hence its portrayal in the media is directly connected to trust in the system of the state.

Key words: Police, media, public, public opinion, trust in the Police, police integrity.

INTRODUCTION

In the past, the Police may not have considered the attitude towards the media as a priority among the many social voices it had to address, but nowadays, it clearly recognizes the potential damage that can be caused as a result of failure to effectively deal with the image the public creates for it in the media. It is clear that nowadays, the media is considered to be essential in building citizens' support for law enforcement and implementing effective police strategies. It is obvious that these public relations strategies demand that the Police meet the conditions for public relations personnel and time devoted to public relations and media. Due to these reasons, police services around the world, including in our country, have established specialized organizational units whose responsibility is to disseminate public information to the media, while simultaneously working on managing the impression of the organization.

Trust and its absence preoccupy and concern us. Trust unites the society in a cohesion and allows people to continue their daily lives. Without it, living in society will become impossible. Often, simply we have no choice but to trust others, but this does not automatically mean that our anxiety is decreasing. Trust is frequently based on our own personal experiences, we use knowledge to form our trust, to decide who and what is considered as confidential.

The public good becomes a kind of special derivative – the concept of an individual who is in the centre of moral and political order. Serving the public good for the individual means serving the phenomenon of social life, in other words, social actors can make strong estimates, for each other, for widespread moral ideas.

Before more than 50 years ago, Marshal made a difference between the political, civil and social component of the public good that he defined as follows: "The civil element is consisted of the right to individual freedom - personal freedom, freedom of speech, thought and faith, right to personal ownership and conclusion of contracts, as well as a right to justice through defence and confirmation of equality with others through established laws." In this definition, the social component of the public well includes a module of economic wellbeing and security, the right to share social heritage and the right to live life as a civilized creature to the standards that prevail in society.

1. RELATIONSHIP BETWEEN MEDIA AND THE POLICE

On a daily basis, police officers are evidently present in the events in the media, either in portals or in TV news. Namely, as the most visible representatives of the local communities, their actions are of great interest to the public and media consumers in the media. Moreover, the various aspects of police work, merged with the public interest in crime, provide enormous media coverage. As Graber, 1980, will point out, news of police work and crime make the vast majority of local and national media issues.

The issue of media representation of police policy makers is related not only to informing for the events or the police work, but also with the penal policy and the state of affairs linked to crime. Media information tights the rules and actions related to crimes and covers much more than organizational issues related to the Police. Policing largely depends on the cooperation in society and the relationship between media, public and police. The presentation of crime and Police in the media is a guarantee for the public`s security and also it creates expectations in the mass media linked to the perception of people for the threat of crime. The impact of the fear of crime is essential and very important for the police organization and therefore the Police must have a positive reputation in the media.

The interest of the Police for building an appropriate relationship with the media is clearly evident, and the media also require their news providers – journalists to have established routine communication about events with official government officials, including official police officials, in order to ensure that they constantly have an authoritative news source. This dependence of the media and journalists on the Police is for the benefit of government agencies and hence affords them a routine status of privileged subjects in the marketplace of ideas, through which they can shape news events to suit their organizational needs.[4]

[4] Jerret S.Lovell (2002), Media Power & Information Control : A Study of Police Organizations & Media Relations, The National Institute of Justice, p.35;

2. THE PUBLIC TRUST IN THE POLICE

The trust should be properly understood, in order to be possible to work on its restoration, or as one of the authors concludes: "In order to restore trust, we need not only trustworthy persons and institutions, but also reasons for evaluating trust and distrust." It is not good to argue for more trust, we need to argue for more adequate trust and for better means of assessing risks".[5]

Trust can be treated and linked to the trustworthiness of a person or an institution, trust is more than a knowledge and trustworthiness is a motive or set of motives for taking action[6]. It is earned based on the motives of the one we trust - we trust because we do believe that the interests of the one we trust include our interests in the sense that the other person also has an interest in the relationship continuing and therefore shall not betray our trust.

On the contrary, trust often seems to be seriously lacking. The extent of the presence of the media in every corner of human life, together with the global spread of information sources through a kind of world wide web, means that it is more difficult to get comfort from the expertise and authority of professionals, politicians and other public figures. Many of us feel that life would be easier, much like in past eras when we felt happy and could get away from some significant figures in our community. Today, endemic cynicism and suspicion, especially within the media, means that our more liberated and individualistic era is not necessarily filled with satisfaction.[7]

Another author gives an important feature of trust, by adding another criterion, such as technical competence.[8] Technical competence is the ability to do what one is entrusted with, in a practical sense. This would mean that the public will trust the Police to be able to promptly identify and find the perpetrator who committed a crime that disturbed and caused fear among the citizens. In this regard, the Police can enjoy trust not only if they are willing to do something, but also if they have the ability to deliver what they promise.

For public trust in the police, it is important to understand the effect of trust as a cause or as a result. What the theory suggests about this effect is that the standard view of trust as a rational effect caused by trusting behaviour is not always very representative of the trust we actually place in objects, people, processes and institutions. The idea of trust, as something we gradually give after carefully observing behaviour and withdraw when we are betrayed, is rooted in the idea of a rationalism that cannot support cooperative and properly trusting behaviour and depends on the use of the wrong method of inference, induction.

It encourages the spread of expectation in gaps, where the standards of reliability that should create trust are really high, and part of this process involves the generation of unconvincing and indisputable narratives of doom that are defined in such a way as to prevent the discovery of counter-evidence. It promotes the use of consultation exercises and authorities trying to do the most popular thing to appear trustworthy. In other words, it is an idea of trust that seems to encourage people to behave in ways that may be counterproductive to fostering trust in general.[9]

---

[5] Onora O'Neill (2002), A Question of Trust: The BBC Reith Lectures, Cambridge University Press, Cambridge, p. 98

[6] Ibid, p. 16

[7] Kieron O'Hara (2004),Trust from Socrates to Spin, Icon Books Ltd, Cambridg, p.9;

[8] Ibid, p. 16

[9] Kieron O'Hara (2004),Trust from Socrates to Spin, Icon Books Ltd, Cambridge, p.256

The standard opinion considers trust as an effect of good behaviour. In fact, that idea can be changed as follows: trust is, or at least can be, a reason for good behaviour. People lean toward trust pretty well automatically, and are surprised when that trust is mispositioned, but they still do not withdraw it easily. Trust should be an act in which the giver does not necessarily expect a benefit, but it is an act of acceptance of the trusted into the moral community.

2.1 Trust as a feature of the social relations

The sociological opinion in the writings of Anthony Giddens (Anthony Giddens, 1971), points out the difference among trust in people and trust in abstract systems. Trust in people is built on mutual reaction and involvement, faith in the integrity of the other is the main source of a sense of integrity and authenticity of oneself. Trust in abstract systems provides day-to-day security, but by its nature it cannot provide the mutuality or intimacy that relationships of personal trust offer.[10] Giddens goes further and relates this difference in types of trust to the difference between traditional and modern society, noting that in pre-modern conditions basic trust is embedded in personalized relationships of community trust, family ties and friendship. Although emotional belonging may be involved in any of these social ties, this is not a requirement for maintaining personal trust. Institutionalized personal ties and informal codes of honesty and honour provide potential, not always real, frameworks of trust.

A greater sociological understanding of the difference between trust and certainty is needed. One of the authors who without a doubt provides the richest set of insights and understandings about trust and makes a very useful distinction between trust and certainty is Luhmann (Niklas Luhmann, 1979). For Luhmann, the difference between the two turns into a difference between risk and danger, between the framing of life's contingencies of an internal or external nature. The key difference between trust in persons and trust in institutions according to Luhmann is related to the progress in the differentiation of the system which makes risk, as opposed to danger, a modern phenomenon, which is also the case with trust. In his words: "Trust remains vital in interpersonal relationships, but participation in functional systems, such as the economy or politics is no longer a matter of personal relationships. Certainty is needed, but not trust".[11]

Trust and certainty are ways to reduce complexity, and in the first instance, trust is necessary for the ontological freedom of the other. The expectation is then generalized that the other will deal with his freedom, with the disturbing potential for different action, in accordance with his personality – or, rather, in accordance with the personality he represents and makes socially visible. However, trust in the proper functioning of the system is different, which is essentially a reliance on the proper functioning of the general communication media. The proliferation of these general media with the increasing differentiation of systems in modernity turns trust into something privatized or subject to psychologism. In modern societies, these forms of relations, at the general social level, are replaced by "systemic trust", that is, predictions based on expert knowledge.

The distinction between trust in people and trust in the system is useful, it is a good starting point, but only a starting point. If we stay in the nomenclature of traditional sociological categories, trust in the system is really nothing more than trust in a set of institutions. The distinction made between trust and certainty then becomes the distinction

[10] Adam B.Seligman, (1997), „The problem of trust ", Princeton Univeristy Press, p.24
[11] Ibid, p.24

between trust in people and trust in institutions. What are institutions, anyway? They are nothing but patterns, embodied normative roles and expectations.

On a historical level, it can be noted that the idea of trust emerged in the modern era as a distinct concern – at least in the form of a concern for finding a new basis for social and political order. The importance of trust and keeping promises at all events seems to be a search for the entrenched social order (what today we would call its institutional or systemic component) and its constitutive acts. Whether it is framed normatively or will be a "fraud" of society, there is a clearly felt need for social life to be based on some external certainty. This need appears with the disintegration of the existing foundations of trust based on common religious beliefs, kinship trust or territorial proximity, that is, the need to root the institutions (system) in something that is above themselves.

For trust in the system, i.e. in its institutions, in the continuous functioning of patterns, normative expectations and roles, institutions cannot be left to themselves, to mediate or limit the flow of resources in the system (in the society). Instead, trust is a flow of resources, it is the system itself (its operating code). What precisely defines a system, what makes system "X" different from system "Y", what distinguishes patterns of generalized exchange, are the different sets of institutions and roles that define the system's goals, desirability, notions of participation, distributive justice and so on. All of these are the system itself because it structures and mediates the flow of resources and when trust is withdrawn from said system it collapses as it seemed to have happened in the Soviet Union and its satellites in 1989.[12]

Fundamental to the definition of trust (as opposed to certainty) is that it involves one in a relationship where the actions, character, or intentions of the other cannot be verified. One believes or is forced to believe, or perhaps it is better to say led to trust, when one cannot know for sure, when one has no authority to detain or check the other and has no choice but to believe. This is seen to be the opposite of that form of reliance, analogous to what following Luhmann above was labelled trust and when, based on one's past knowledge (or sometimes one's ability to impose future sanctions in the event of "betrayal") or future opportunities for "verification" (similar, in a sense, to sanctions), one can rely on or trust the other's words, commitments, or actions. Trust, then, involves vulnerability caused by some form of ignorance or basic uncertainty about the other's motives.

We can speak of trusting a person's opinion (which can be uncertain), not trusting his knowledge (which can only be what it is); we claim to trust a person's choices (which can go either way), not to trust such completely determined behaviour (in principle thoroughly predictable) as his reflexes or heart rate.[13] In short, it seems that trust is most needed precisely when we least know whether a person will or will not do something.

Following social roles, normative role expectations and roles institutionalized within interconnected system activities as a function of the social system are another aspect related to the existence of trust in social relations.

Understanding social roles through the description of role-taking in terms of process is part of the sociological tradition. Here, roles emerge from interaction, are less determined by system constraints, and essentially their function is more reciprocity between role holders. Trust enters into social interaction in the interspaces of the system, or at the limitation of the system, when for one reason or another the expectations are no longer achievable for the systemically defined roles. By defining trust in this way, we succeed in isolating the

[12] Ibid, p.33
[13] Ibid, p.33

phenomenon of trust from a reduction of faith or belief on the one hand, or from trust in the fulfilment of role expectations on the other.[14]

Whether we have in mind expectations for the survival of a moral social order, expectations for technically competent performance, or expectations for trust in responsibility, we must always specify social relations or a social system. What counts as competence or confident responsibility among friends may be different from trust in families, and of course both types are likely to differ from that in a work organization or society as a whole.

Different social systems, at the same level of generality or systems at different levels of generality, have different expectations related to trust.

3. FORMS AND THEORIES OF ACQUIRING PUBLIC TRUST

We can trust different things, not only people, but also animate and inanimate objects, systems and institutions. We believe that our physical environment is more or less constant and plastic. The extent of our trust, who and what we trust and why, to what extent and in what field, really depends on a wide variety of factors. Why should we care about trust, and why now? On a number of fronts around the world, trust has become a problem in politics and in the conduct of public affairs.

Trust may have a moral dimension, or morality may be absent. If we return from vacation and find that our apartment has been burgled, we will report the theft to the police station and trust that the police officers will do whatever is necessary to find the perpetrator and that they will not be stuck with some other problem that would affect the perpetrator is not detected. This is not a moral claim – it is an expectation of their ability. On the other hand, if we pay someone to do something in advance, then they are morally bound to perform the task to the best of their ability, and we trust that they will do their duty in this regard.

Let us take a really trivial example: we walk into a police station with a request to get a new personal identification document. Our beliefs are simple, the police officers know the procedure, they know what checks they need to do in order to guide us on what to do next. The procedure is simple, we say the request, and then the procedure is explained to us and we follow the steps. We believe that the police officers will explain everything necessary to get the new identity document. We do not have to think about what to say, we believe that the police officers know what they are doing and we expect to receive the identity document after completing the procedure. Securing new identity documents is becoming routine.

Our trust in the role of police officers, and fulfilling that trust together, make the world much more stable and predictable. This is a type of socially based predictability. Because we have this mutual trust in each other's goals and understanding of our interactions, we can build society around such institutions as the Police, the post office, stores, or whatever. Trust makes achieving our goals more likely. In the dark jargon of the new century, it is an enabler, a facilitator.

Another aspect through which the Police gains trust is cooperation. If two people are to engage in any kind of collaboration, they will need to trust each other. When a winger passes the ball at the right height in the penalty area, he trusts that the centre-forward will be there to take a header, and when the centre-forward runs down the middle, he trusts that the winger will get a decent cross. If either player does not trust the other, the action will break down. Similar to actions in sports, the Police take coordinated actions in public, which are

[14] Ibid, p.35

often reported in the news or broadcast on television or other video footage of the scene. Police officers should show coordination and an appropriate degree of synchronization in the implementation of actions, show mutual trust in acting and taking measures in order for them to be successful and to take control over the events or, in the last case, to establish a safe environment the place where the action takes place. Any plan that involves two or more people working together, from cooking Christmas dinner to assembling a library or building an oil platform, requires mutual trust in the mutual capacity and willingness of those working together to get the job done.

3.1 Public trust and the legitimacy of the Police

The idea that institutions should provide security, and in return gain legitimacy of their authority, tries to underpin trust with contractual or quasi-contractual relationships. Trusts and contracts are very analogous, although they operate in different contexts and have slightly different properties. Indeed, some studies show that the development of trust is inhibited by binding contracts. When a binding contract governs a particular relationship, the parties tend not to foster trust, leaving it to regulate acceptable behaviour within the relationship itself. The contractual tradition may need to be adapted to the facts of human behaviour.[15]

Public opinion about the Police, public trust and its legitimacy are important for the performance of the Police's function. The role of the media is significant for all societies, but the role of the media in democratic societies has a higher level of importance. The media has the power to create reality and therefore its role in modern societies is important. They affect our perception of the world around us. If we want to be informed about the various events, the only possible way is to get some sort of summary through the mass media. Their role is greater than the transmission of messages from sources to receivers. They are constructors of social reality.

The media influence the image of the Police and the formation of public trust in the Police. Thus, the public assessment of police effectiveness depends on media reports of police activities. In cases of major crime stories that the media focus their attention on, police activities are evaluated at different stages, and such information related to some events appears and is present in the media long after the event itself has occurred.

The Police must know that the public and the media are partners with whom an appropriate relationship of cooperation should be built for the sake of mutual interests, and the recommendations would be in the direction of striving to achieve the ideal relationship which should contain the three basic elements – transparency, efficiency and trust in the Police, which are also in the interest of the three parties – the Police, the public and the media. Transparency, accountability and respect for the basic principles of human freedoms and rights by the Police are in the interest of both the citizens and the Police.

[15] Kieron O'Hara (2004),Trust from Socrates to Spin, Icon Books Ltd, Cambridge, p.62

CONCLUSION

Recognizing the need to maintain public trust is key to effective policing, many police services have begun to incorporate media skills as part of their training protocols in preparation for dealing with "ambush interviews", appropriate behaviour in difficult situation, as well as to achieve success in generating good media coverage of police work. On the other hand, such a system is very dependent on the mass media that spread the word, on the politicians and officials of the institutions that appear on television, in the shows and news of the national media. Given that the media is a key mechanism for filtering information, through reputation, the bearer of trust (which is ideal for public life) is created from a filtered set of a potentially infinite number of events and activities.

If the central question for the work of the media revolves around the public interest, then in the sphere of competence of the Police and its work, we can put the public good, which as a concept has vital importance for the functioning of society.

BIBLIOGRAPHY

Bradford, B. & Jackson, J. (2007) "Policing into the Future, Police Legitimacy in Action: Lessons for Theory and Policy", Oxford

Jerret S.Lovell (2002), Media Power & Information Control: A Study of Police Organizations & Media Relations, The National Institute of Justice;

Kieron O'Hara (2004), Trust from Socrates to Spin, Icon Books Ltd, Cambridge;

Onora O'Neill (2002), A Question of Trust: The BBC Reith Lectures, Cambridge University Press, Cambridge;

Adam B.Seligman, (1997), "The problem of trust", Princeton University Press

UDK: 355.02:004.7

IMPACT OF CYBER SPACE ON SECURITY IN THE CONTEXT OF ARMED CONFLICTS: TOWARDS DISASTER RISK RESILIENCE

Dalibor Milenković
Scientific-Professional Society for Disaster Risk Management, Belgrade, Serbia;
International Institute for Disaster Research, Belgrade, Serbia;
milenkovic.dalibor82@gmail.com;
Vladimir M. Cvetković
Department of Disaster Management and Environmental Security, Faculty of Security Studies, University of Belgrade, Serbia
Safety and Disaster Studies, Department of Environmental and Energy Process Engineering, Montanuniversität of Leoben, Austria;
vladimir.cvetkovic@unileoben.ac.at.
Aleksandar Ivanov
Faculty of Security – Skopje
University St. Kliment Ohridski Bitola, North Macedonia;
aleksandar.ivanov@uklo.edu.mk.
Renate Renner
Safety and Disaster Studies, Department of Environmental and Energy Process Engineering, Montanuniversität of Leoben, Leoben, Austria

Abstract

The rapid evolution of cyberspace has profoundly impacted security dynamics and the conduct of armed conflicts. As an integral domain in modern warfare, cyberspace intertwines with traditional conflict factors, such as human and material resources, space, time, and information, redefining their roles and interactions. This paper explores the influence of cyberspace on security within the context of armed conflicts, highlighting its dual nature as a battlefield and a tool for shaping strategic outcomes. Emphasis is placed on integrating advanced technologies, including artificial intelligence and the Internet of Things (IoT), in enhancing operational capabilities and addressing hybrid and informational warfare. Furthermore, the study examines the critical role of disaster risk resilience in mitigating the cascading effects of cyber-related disruptions during conflicts. The findings underscore the need for a comprehensive approach combining technical innovations, organizational strategies, and robust regulatory frameworks. The paper concludes that achieving resilience in cyberspace requires multidisciplinary collaboration, continuous capacity building, and the alignment of security policies with emerging technological challenges. The findings highlight the critical importance of integrating digital infrastructures, regulatory frameworks, and innovative technologies, such as artificial intelligence and the Internet of Things (IoT), to mitigate cascading effects during armed conflicts. By emphasizing adaptive strategies and capacity-building, the paper offers actionable insights for policymakers and practitioners aiming to strengthen societal and infrastructural resilience in the face of hybrid threats.

Keywords: cyberspace, security, armed conflicts, disaster risk resilience, hybrid warfare, artificial intelligence, Internet of Things, regulatory frameworks, operational capabilities, resilience building.

1. **Introduction**

Civilizational development viewed through the prism of technological progress and the improvement of comprehensive social relations, along with the constant striving for something new, as the basic determinant of all modern states, imposed the necessity of dealing with often completely new fields, that is, the circumstances in which organized societies must function (Friedmann, 1952; Kolganov, 2022; Stepanyants, 2022; Zgirovskaya, 2023; Ноономика et al., 2022). The pursuit of progress imposed the need for an intensified connection of all social segments that in the past were even separated and distant by default. It was the merging and synchronization of certain social segments that contributed to an even greater acceleration of progress, to which even developed countries often failed to respond adequately and cope with the changes completely successfully.

The acceleration of all processes in modern societies has created a sense of constant tension or friction between what has become old and what is considered new. The answer to these circumstances is to define such a situation as a crisis. It is precisely the increasingly frequent crises that impose conflicts as a response. War, as the ultimate origin of social conflicts, aims to change and impose the will, i.e. the continuation of life in new circumstances imposed by the winner. In the recent past, the will was imposed by the concrete disintegration of the adversary or its resources.

Today, imposing a will and changing circumstances does not require such brutality as was used in the previous period (Alemzadeh, 2023; Bandura, 1999; Dobash, Dobash, Cavanagh, & Lewis, 1996; Hall, 2018; Hubert, 2017; López, 2020; Schinkel, 2004; Townsend et al., 2023; Urbatsch, 2021; Van Swol, Prahl, MacGeorge, & Branch, 2019). All-out destruction of opponents is becoming less necessary but is still often the key way to resolve social conflicts. Precisely because of this, the perception of war is actively changing, and its conduct is increasingly influenced by completely new segments in social development. Societies that perceive the impact of new circumstances go to meet them. Some societies, instead of action, function on the principle of reaction when a new circumstance causes problems or damage, which can often be irreparable.

Especially because of the above, i.e. the evolution of the classic military conflict as a way of conflict resolution, it is necessary to look at certain new segments of social development with the factors of armed struggle, which represents the basic content of war. In the context of the above, information and communication technologies (ICT) can be considered as new segments of social development, i.e. cyberspace itself is viewed as a place where certain elements of the factors of armed struggle, reflected in human and material resources, space, time and information, are intertwined.

In the context of disaster risk resilience, the integration of cyberspace and its associated technologies plays a crucial role in mitigating the cascading effects of armed conflicts on societies (Cvetković & Šišović, 2024; Milenković, Cvetković, & Renner, 2024). Resilience is not solely about enduring disruptions but also about adapting and thriving amidst challenges. Cyberspace, as a domain, offers unprecedented opportunities to enhance early warning systems, optimize resource allocation, and ensure the continuity of critical functions during conflicts. By leveraging innovations such as artificial intelligence and the

Internet of Things (IoT), this paper emphasizes the potential of resilient digital infrastructures to protect human and material resources, preserve critical information, and maintain societal stability. This aligns with the broader objective of fostering adaptive capacities and reducing vulnerabilities in the face of hybrid and technological threats.

The aim of this paper is to explore the impact of cyberspace on security in the context of armed conflicts, with a particular focus on disaster risk resilience. By examining cyberspace as a pivotal factor in modern conflicts, the study analyzes how technological innovations, such as artificial intelligence and the Internet of Things (IoT), can contribute to the resilience of communities and infrastructure against the destructive effects of conflicts. This underscores the necessity of integrating technical solutions and risk management strategies to enhance resilience and mitigate the effects of hybrid and informational threats in contemporary society.

2. Characteristics of modern war

War has always been one of the ultimate ways of resolving conflicts between two social entities (Cvetković, 2024a, 2024b; Cvetković & Šišović, 2024; Grozdanić & Cvetković, 2024; Tanasić & Cvetković, 2024). Although it has traditionally been expressed throughout history as a desire to physically destroy the opponent in any form and then impose one's will, it also implied other aspects of social conflicts, which, however, were not so efficient and effective. Therefore, looking at earlier periods, wars can be divided into several eras. According to the character of armed struggle and its evolution, William Lind and George Thiele (Lind & Thiele, 2015) formulate the division of wars into four generations with all the specificities that these generations carried.

Roughly speaking, under modern, or fourth-generation war, we can consider those that have taken place in the last three decades, that is, in such a way that a neutral observer who is a layman can notice all the changes compared to previous wars and conclude certain regularities. This does not mean that in the previous historical period, what was sought in wars from the recent past was not sought, but that at that time there were no objective possibilities and knowledge to realize these aspirations.

A characteristic of the wars of the last generation is the complete involvement of all segments of society in the war. This is understood to mean that the entire population and territory of an entire country or region are involved in the conflict, along with all the available resources that a society or country has at its disposal. Such conflicts, due to their comprehensiveness and asymmetry, are considered and called hybrid wars. This form of war involves a set of actions that can affect certain segments of society and influence the outcome of the armed conflict. "The rise of this type of conflict does not represent the end of conventional warfare, but it is a factor that greatly complicates defence planning in the 21st century." (Hoffman, 2007, p. 9).

Hybrid warfare involves armed conflict that simultaneously involves military and non-military means intending to direct the enemy towards activities that he would not voluntarily undertake" (Hybrid Warfare: A New Phenomenon in Europe's Security Environment, 2016, pp. 10-11). The main role in hybrid warfare belongs to several subversive activities through special operations, combined with economic or commercial pressure. Moreover, in addition to regular military operations, those that are considered irregular can also be used. All activities can be directed both at the entire society and at individuals or certain segments of society, such as political structures, state bodies or the

enemy's armed forces themselves (*Hybrid Warfare: A New Phenomenon in Europe's Security Environment*, 2016).

3. Factors of armed conflict

The understanding of what constitutes a modern army is closely linked to the circumstances and factors surrounding the defence system in a society and its immediate and broader international environment (Creveld, 1992; Gareev, 2001; Kier, 1995; Kristoferson, 1981; Milinovic & Ivaniš, 2015; Santala, 2004; Westing, 1988; Wilén & Strömbom, 2021). A proper understanding of the relevant circumstances and factors is a prerequisite for quality planning of the use of armed forces, which demonstrates its affirmation through effectiveness in practice during the execution of the basic assigned tasks. The armed forces of a modern country, in addition to the capacity for immediate use, in the current circumstances must also represent a factor of deterrence and prevention that is used together with other social segments.

To implement this, the armed forces must have achieved the desired operational capabilities. For what is considered operational capabilities, the definition in the Serbian Army can be taken as an example, which states that they represent the ability of the army or its parts to achieve the desired operational effects, within a given time and under certain standards and conditions, by combining forces, means and methods of performing tasks (Serbian Army, 2022). However, classic war, manifested by armed conflict as a basic phenomenon, has remained the main ultimate way of imposing the will of one side on the other. The use of organized armed violence and its nonlinearity and asymmetry is a consequence of the different overall levels of development of the conflicting parties. The goal is to inflict as much damage as possible on the enemy and deviate from the rules of combat that are imposed.

Armed struggle, as a fundamental element of war and armed conflict, is a way to cause changes through combat actions that imply political, economic, military and other goals. Armed struggle is characterized by duration, hierarchy, intensity, manoeuvre, interdependence and coordination. The course and outcome of armed struggle are influenced by the following factors: human resources; material resources; space; time and information. Here, the context of the elaboration of the aforementioned factors, which in this case are closely related to armed struggle, must be particularly taken into account.

Human resources, as in the civilian sector, are today becoming a decisive factor for the successful functioning of the armed forces. Adaptive management of this resource in times of constant changes in use but also in living and working conditions requires monitoring of needs, demographic and economic potential. They include the demographic capacity of the country that can be used effectively for military purposes in an armed conflict. The term effectively means their exploitation to a reasonable extent and in a way that optimally utilizes the potential of each individual.

Material resources today represent the most complex factor of armed struggle. They encompass the entire social potential reflected in natural, industrial, financial, energy information and communication potentials. Planning, construction, use and resilience of the above segments of material resources represent a basic prerequisite for armed conflict or its prevention in terms of building a deterrent factor about a potential adversary.

Space as a factor in the classical sense represents the place where armed struggle is waged. Space includes land, sea and air. In the past, these three segments of space were a

limiting factor and were largely defined by the line along which armed struggle took place. Today, in modern conflicts, these three segments of space include not only what is possessed by the two entities in conflict, but also wider parts related to foreign or international space. In this context, the most developed countries in the world consider space as one of the physical segments of space and actively exploit it. In general, there is no clear marking of the space in which armed struggle is carried out, there is no background or depth of territory that would be inaccessible to the enemy.

Time as a factor of combat manifests itself as a determinant of the duration of an activity, as the time of day or year, or as a meteorological phenomenon. In the modern context of armed conflicts, time becomes an essential resource and all processes in armed conflict are drastically accelerated, which is why the flow of time often becomes a decisive factor for the implementation and conduct of armed conflict. In addition to the above, in terms of meteorological conditions, time becomes a less significant factor with the application of more advanced technologies, i.e. the limitations for conducting armed conflict are becoming smaller.

Information as a factor implies the availability of knowledge and data necessary for the successful conduct of armed conflict. Possession of the necessary information reduces the uncertainty of the successful implementation of necessary tasks. Possession of quality information in the required period enables the successful achievement of set goals or the prevention of undesirable outcomes. The specific feature of information as a factor is that it has the greatest degree of interaction and influence on other factors of armed conflict. It represents a vital resource that is the product of the collection, processing and exchange of data on other factors of armed conflict (2010).

4. Cyberspace

Technological progress, especially in developed countries, is often closely linked to development projects of the army or defence system in a broader sense (Chkhikvishvili & Beridze, 2024; Dexia, 2012; Gilli & Gilli, 2019; Herolf, 1988; Howe, 2006; Kupchyn, Dykhanovskyi, & Kolotukhin, 2020; Pysarenko et al., 2024). The development of each new detail is always placed in the context of its impact on the ability to defend or threaten society, regardless of what is meant by the defence. Every technological "breakthrough" in a certain scientific field always has an impact on the context of material resources as a factor in armed conflict. The acceleration of development and the complementarity of new knowledge and products have created the interpenetration and interdependence of all parts of society, where the development of ICT plays a special role in connecting them. The emergence of ICT and their development have completely changed the classic armed conflict, both directly and indirectly. Directly because they have changed and are changing the degree of influence of the factors of armed struggle or conflict, and indirectly because they change the perception of armed conflict, the need for its intensity, purposefulness etc. Because of the above, Putnik states that "information and communication technologies have a special influence on the beginning, course and outcome of the conflict." (Путник, 2022, p. 42).

Throughout history, the development of ICT has had various impacts on armed conflict. The impact has changed over time, becoming more complex and multidimensional. More complex, because it initially enabled faster transmission of messages, and with later development, it began to affect all factors of armed conflict, while today it has its unequivocal great impact on all flows before, during and after armed conflict. To be precise,

it permeates the entire process of relations between two opposing entities, where armed conflict is only one of the phases of conflict resolution. This has also been contributed to by the availability of technologies throughout the world, where the advantage of using ICT is no longer only for richer societies.

As a consequence of the presence of ICT and its development, the term cyberspace has been actively used since the beginning of the 21st century (Babulak, 2010a, 2010b; Chatinakrob, 2024; Kellerman, 2010; Lan, 2021; Mbanaso & Dandaura, 2015; Muller, 2015; Sim, 2023). It generally refers to electronic communication networks that are connected to devices or groups of interconnected devices that have the property of automatic operation using computer programs (Information Security Act, 2019). Initially, the perception of cyberspace as a segment in which conflict can be waged or a type of space that can affect the armed conflict itself was not given much importance, primarily because there was no awareness of its use or the consequences of its use. Technological development has influenced cyberspace to expand and enter every socio-societal activity, from the life of an individual to the use of the most complex means of warfare.

The doctrines of the most militarily developed countries in the world and military alliances have placed cyberspace on the same level as land, sea, air and space (North Atlantic Treaty Organization, 2022). It has become a place for defence but also a place or means for attacking the enemy. Accordingly, the last two decades have marked a period of the emergence of military "cyber capacities", which were reflected in the development of human and material capacities for conducting cyber activities (protection and attack). Just as classical forces (army, navy, air force) have developed, so too has the continuous development of military cyber capacities been noticeable. It can be said that they are not only complementary to other types of military but that they are becoming an element that permeates through the aforementioned classical types and that this interpenetration becomes their "bloodstream", without which they will not be able to function shortly.

The US Department of Defense's definition, in the context of armed combat factors, even more closely states (clarifies) that "cyberspace is an area in the information environment consisting of independent networks of information structures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers." (*Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, 2016, p. 58).

Due to the above, it is particularly important to emphasize that the perspective of cyberspace in the future is to cease to be a segment of space as a factor of armed struggle and to become one of the key independent factors of armed struggle.

4.1. Cyberwar

Information as a starting point in any military armed conflict or battle represents the essence and potential to win or avoid defeat (Bogdanoski & Milkovski, 2015; Johnson et al., 1997; Libicki, Gompert, Frelinger, & Smith, 2007; Neculcea, 2021a, 2021b; Reese, 2020; Serrano & López, 2008; Toroi, 2021). For a set of objective facts, converted into data and shaped into information, often in the past, more important than the quality itself was how quickly it would reach the user who makes decisions in the conflict. With the development of technologies that enabled two-way and one-way communication, information consumers were born and developed. It is easiest to divide them into two groups, primary, those for whom the information is important for decision-making, as well as secondary, for whom the

information is of less direct importance, but who ultimately decide on the course of events (conflict).

During the 20th century, if we exclude the standard two-way communication channels for command in conflict, the most important step was made in one-way communication channels towards the ordinary person, embodied in radio and television. The importance of these two forms of communication was quickly recognized and exploited to the extent that it has often played a decisive role in influencing all aspects of armed conflict, before the conflict as preparation, during the conflict to shape it, and finally to indicate the achieved goal and purpose of the completed conflict.

The end of the last century and the beginning of the present century brought the possibility of instant two-way communication between the recipient and the sender of information via computer networks in the broadest sense of the word. The possibilities of this type of communication and its fundamental importance were not understood by many countries or societies even in the second decade of this century. In addition to the above, comprehensive social development has integrated ICT into all aspects of the functioning of a state, to the extent that almost everything functions when it is "on a network". This fact has not bypassed more complex systems or means of military technology in modern armies, where in addition to the transmission of information, the newly created space enables the autonomy of the action of these means and their implications for the physical world.

There are still active scientific debates about establishing and defining a term for the newly emerging space, or rather the conflict in it, that would be generally accepted and that would shape the relevant topic. Thus, Putnik and Milošević state that cyber warfare is a continuous conflict between national armies or guerrilla groups in cyberspace, which involves conducting attacks on the opponent's information infrastructure using malware and other cyber tools and techniques, as well as conducting propaganda activities, to cause damage to the opponent and weaken his defensive capacities in the cyber and physical world (Putnik & Milošević, 2018). The above definition represents the sublimation or genesis of a larger number of definitions, primarily modern military ones, that treat the concept of cyber warfare.

The essence of cyber warfare is that it takes place in a space that is separate and distinct from the others that are incorporated into the classical space as a factor of armed combat. It is also characterized and shaped by the computers and computer networks in which it can take place.

4.2. The impact of cyberspace on the factors of armed conflict

Modern armies and military alliances have become increasingly aware of the advantages and dangers that cyberspace brings with it in its current state of development. That is why, in the first decade of the 21st century, they placed this type of space on an equal footing with other segments of space as a factor in armed conflict (National Security Strategy, 2022). They began to actively develop human and technical capacities for defensive and offensive actions in cyberspace. Initially, these were smaller units, almost experimental in nature, today they are equal formations with organizational structures and a way of functioning that is almost the same as in other types of armies. Regardless of all the facts and objective circumstances, there are still armies that strive to be modern, but do not have defined, regulated and rounded cyber capacities in their formations. It can be said that these compositions are in experimental stages and that they are a full decade behind objective reality and the needs of the future.

In the militaries of states that are facing future circumstances, there is a noticeable tendency to expand cyber capabilities in such a way that they become integral parts of other classical aspects in a single army or military alliance. Their role and complementarity are becoming an indispensable factor and prerequisite for the successful use of armed forces.

Considering the influence of the factors of armed conflict, with their mutual intertwining, on the course and outcome of an armed conflict, it is necessary to consider in what ways cyberspace as a place of cyberwar can individually influence each factor of armed conflict. First of all, it should be taken into account that two types of cyber operations take place in cyberspace: internal, which relate to security and defence, and external, which relate to attack or exploitation of cyberspace. ("Cyberspace Operations," 2018). „Cyber operations are the use of cyberspace capabilities to achieve objectives in or through cyberspace.“ (*Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, 2016, p. 58).

When it comes to human resources as a factor in armed conflict, the influence of cyberspace can be divided into two segments. The first is the one that precedes the armed conflict itself in which the goal is to obtain enemy data or to protect as much as possible of one's data about individuals or the entire human resources of society that are available for armed confrontation with the enemy. Today's functioning of each individual is unthinkable outside the virtual world where, intentionally or not, a huge amount of data is left behind that can be used to reach conclusions, or information that can be used or be of key importance for the outcome of an armed conflict.

In addition, cyberspace allows for the manifestation of an immediate and constant influence on the enemy's human resources, but also on one's people, which can change things on the ground in an instant. The second segment of influence is the one that is realized during the immediate armed conflict. The goals are the same as in the first segment, but with a far greater influence of other factors of armed struggle, where, primarily due to the acceleration of the flow of information, the processes of influencing human resources are simplified and accelerated, all to collect data on people as quickly and easily as possible and reach individuals who will receive the data or information with an easily understandable message, which will influence them, a group or the entire composition of the enemy.

Due to all of the above, a very important prerequisite for building human resource resilience in modern armed forces lies in raising awareness and educating personnel, clear and precise regulations, and internal cyber operations that will increase security, enable the flow of information, and exercise control over cyberspace.

Material resources, as the most complex factor of armed struggle, are directly related to the level of development of a particular society. Also, the achieved level of development of a society unambiguously indicates the impact of cyberspace on material resources, primarily because they represent the entire potential of society sublimated into natural, industrial, financial, energy and ICT capacities. Any modern society is capable of waging an armed conflict only if it has built high-quality and comprehensive resistance of the aforementioned segments, but also the ability to constantly threaten enemy material resources with its capacities.

One of the segments of this resilience and capability is the protection and threat of this factor of armed struggle in cyberspace. This is primarily important because today, both in peace and in war, almost no segment of material resources can be used or used for defence without being in some direct or indirect connection with cyberspace, whether it is coal mining or the use of the latest means of warfare. The resilience of material resources in

cyberspace is ensured by striving for optimal autonomy, clear and precise regulation, improvements and raising of the work safety culture, and comprehensive cyber operations to increase the security and control of cyberspace.

In every armed conflict, space as a physical phenomenon is divided into several entities (land, sea, air, space). In the past, these entities were divided and had less mutual influence. With technological progress, the entities of space became complementary, with greater interaction, that is, the growth of mutual influence. Today, armed conflict cannot be imagined and waged without the absence of some of the entities of space. Cyberspace, unlike the aforementioned physical entities, has become a place where the entire physical space is unified. Today, it is not possible to wage a modern conflict without the existence of technologies that are connected to such an extent that systems must be developed that help other systems distinguish who is the enemy and who is the friend during the conflict (Identification, friend or foe – IFF), and in what can be called the space of armed conflict. In recent decades, cyberspace has contributed to the loss of a clear definition of space or one of the entities of space, or rather, to the absence of its clear boundaries. It has become irrelevant where and what the "background" is and where the depth of the territory, one's own or the opponent's, is.

The successful functioning of the armed forces in space, and the resilience of the synchronized use of all its components, are conditioned by the capabilities in cyberspace, primarily in the application of a set of state-of-the-art technologies for protection, but also the possibility of unhindered use of all systems that improve the complementarity of the use of military equipment in all components of space. Here, as with the previous factors, legal regulations must be taken into account, as well as the scope of cyberspace used by the armed forces, the security of the aforementioned scope, the development of ICT and the ability to use it.

Time in the context of armed conflict factors manifests itself in many ways. As a determinant of the duration of an activity, as the time of day or year, or as a meteorological phenomenon. Considering that the most important part of this factor is time as a determinant of the duration of an activity, it is easy to conclude how much cyberspace has contributed to the acceleration of activity during armed conflict in recent decades. In earlier times, activity was often conditioned not only by information but also by the speed of its distribution. Often, some of the active actions were implemented in a short time, but the path to it, primarily waiting for the exchange of data, took the most time and therefore the conflicts lasted longer, with a lower degree of loss of effectiveness (people and equipment). Today, with the development of new data transmission technologies that take place in real-time, the duration of armed conflict has been drastically reduced, but also the effectiveness and efficiency of the use of military equipment have been increased, which in turn has greatly contributed to conflicts ending earlier due to the accelerated loss of human and material resources.

Information as a factor of armed struggle represents the availability of knowledge and data that are necessary for success in a conflict. In addition to the speed of availability of certain information, which is considered timeliness, possession of the necessary reliable information is a prerequisite for victory or avoidance of defeat. The specificity of information lies not only in its complementarity with other factors but also in the fact that in a modern conflict, it has perhaps the greatest influence on the outcome of the same. Information itself is created by collecting, processing and exchanging data on the facts of one's own and enemy factors of armed struggle. It is precisely the development of cyberspace

that has enabled the exponential rise of information as a key element for a successful positive end to the conflict.

The development of ICT has enabled, in addition to accessibility, the storage and processing of available information. This has contributed to a change in the balance of power between individual states, because it has made the disposal of military resources in the classical sense less competitive. The war for information, through information and against information in cyberspace itself has in many ways made classical armed struggle much more complicated to wage. Putnik states that "the mastery of information and the establishment of control over it have promoted it into the basic object of cyber warfare, and cyber warfare into the primary form of conflict. Victory in the war for information has become a prerequisite for victory in a traditional military conflict" (Putnik, 2022, p. 90).

Building resilience in the handling of information, its distribution and exploitation represents, in addition to material resources, not only the most complex but also the most important prerequisite for the successful conduct of armed conflict. The set of measures, actions and procedures that must be taken with this goal requires the mobilization of all available resources. The above implies investment in technological progress, the autonomy of ICT systems, comprehensive legal regulation, the security aspect in the broadest sense, but also internal and external cyber operations of the defence system during an armed conflict ("Cyberspace Operations," 2018).

5. The impact of artificial intelligence on the factors of armed struggle

The development of science in most parts of the world is closely linked to military or security issues. Very often, it is the armies that become the first users, even experimental ones, of the latest inventions in science. Putting cyberspace about the factors of armed struggle, it is very easy to conclude that it is precisely military elements that are the actors in the implementation of a large number of activities in cyberspace, which to a certain extent are also characterized as cyber attacks on other entities, broadly speaking.

Modern armies have been actively using artificial intelligence as a tool for working in cyberspace for many years. The reason for using artificial intelligence for military purposes lies in its recognizable definition as a device or set of connected devices that can implement activities that require human intelligence (Galan, Carrasco, & LaTorre, 2022). Although there are levels of artificial intelligence in theoretical considerations, today the artificial intelligence that has segmented capabilities in one field for which it is specialized is still used in practice. Currently, the factors of armed combat abound in enormous amounts of data, be it human resources, material resources, information, and even time as a factor with all its constituent segments. The above data represents an area where, among other things, modern armed forces use artificial intelligence to process this data and obtain conclusions that require the same quality as if a human had analyzed it with his intelligence.

Due to the speed of arrival, quantity and diversity, traditional methods of storing and working with data, such as relational databases, have been replaced by artificial intelligence that allows for almost instantaneous processing of the same. The essence of large amounts of data is not only in processing and analyzing it, but also in predicting and influencing the future with it (Cintiriz, Buhur, & Sensoy, 2015). If data of importance to the armed forces are divided by source, we can classify them as: public (government and public administration); private (legal entities and individuals); data from social networks; secondary data and data on the behaviour and actions of the entity. During an armed conflict,

in addition to the above data sources, a huge number of specific data are obtained from intelligence and reconnaissance activities (George, Haas, & Pentland, 2014).

Modern armed forces use large amounts of data for direct and indirect needs. When it comes to direct needs, these are: familiarization with the intelligence situation and knowledge management; knowledge of the operational situation; decision-making process; cyber defence and attack; information management; military forensics, and geographic information systems. The indirect spectrum of needs is broader and more comprehensive and refers to more complex terms, namely: conventional warfare; counterinsurgency actions; hybrid warfare, asymmetric threats; counter-terrorism; logistics; command and control operations and technology development for military needs (Cintiriz, Buhur, & Sensoy, 2015).

Data processing for the above direct and indirect needs is performed using machine learning. "Machine learning is a branch of artificial intelligence and computer science that focuses on using data and algorithms to imitate the way human learning works, gradually improving its precision or accuracy" (www.ibm.com, 2017). Data processing in this way is necessary not only because of the shorter period until conclusion but also because it processes a large amount of data independently or with minimal human corrective role in the processing process. Machine learning allows for the detection of difficult-to-see logical patterns in data. If we consider the sources of data, their volume, and the needs of the armed forces that can be met by them, the most common areas in which machine learning is applied for military purposes are:

- Combat platforms – They include complex combat systems such as armoured infantry systems, vessels, aircraft, artillery and missile systems, anti-aircraft defence systems etc. Their characteristic, which are achieved by machine learning, is minimal human intervention during operation, better synergy of all subsystems, and reduced need for maintenance, which collectively implies improving the autonomy and firepower of these assets;
- Cybersecurity of defence capabilities – These capabilities mainly include systems for command, control, communications, computers and computer networks, systems for collecting intelligence, reconnaissance and surveillance, as well as systems for finding, tracking and selecting enemy threats and targets. Machine learning enables the automatic protection of networks, programs and data they use from unauthorized access. In addition, they monitor cyber-attack patterns and develop counterattack tools;
- Logistics and transport – This area uses applications that enable the optimization of defence logistics and transport systems. During armed combat, it is crucial to make the optimal allocation of material resources, military equipment, ammunition etc. The implementation of machine learning in this area enables timely supply, cost reduction and engagement of the human factor. The use of machine learning is also used at the tactical level, which, for example, in the US armed forces allows for the prediction of necessary maintenance and the prediction of failures in armoured combat vehicles;
- Systems for finding, tracking and selecting threats and targets – In addition to being used for their security in cyberspace, machine learning is also used to understand the zone of operation, through the analysis of intelligence, reconnaissance and other reports, documents and other forms of information obtained from a large number of integrated sensors of various nature, which is a prerequisite for situational awareness on the battlefield, i.e. finding, tracking and selecting threats and targets. These systems are

multidisciplinary in nature and are used by all types of armed forces. They are mainly integrated into combat platforms;

- Medical support – Autonomous platforms are used on the battlefield to extract wounded members of the armed forces, and their further medical care, as well as for rapid identification of injuries and diagnoses in combat conditions;
- Training – It involves the use of platforms for exercises through computer simulations and the use of combat platform simulators. Machine learning, through these two platforms, allows the creation of a completely realistic situation for personnel training. In this way, more comprehensive training is achieved for different types and conditions of force engagement and drastic savings of money and time for training purposes are achieved; (Abell, 2020).

In order to be able to round off the issue of the influence of cyberspace and artificial intelligence on the factors of armed conflict, it is necessary to take into account the tendency of development of the so-called Internet of Things (IoT), their connection with cyberspace, the role of artificial intelligence and the further perspective of their use in armed conflicts (for military purposes). Specifically, "the Internet of Things represents an interdisciplinary technology that connects networks, embedded hardware, software, sensor technologies, information management, data analysis and visualization in a single object, while the term thing refers to any controlled device that can be communicated with at a distance and that can collect data (Suri et al., 2016).

The essence of the functioning of IoT is in networking, or the use of networks, therefore their influence permeates all factors of armed combat almost evenly and therefore will not be considered individually for each factor, but rather the focus is on their definition and analysis by certain factors. Currently, modern armed forces mostly use IoT for C4ISTAR systems, which means: command, control, communications, computers, intelligence and surveillance, target selection and reconnaissance. In parallel with the use and procurement of these systems, in recent years, a fifth letter "C" (C5ISTAR) has been added to them, which implies cybersecurity of the use of the system. In other words, IoT for these purposes is improved with a component that enables safe use in cyberspace to the extent possible (www.adsinc.com, 2021). The aforementioned system involves the integrated use of a larger number of devices and platforms. These are networked communication and information devices and platforms (communications means); multi-sensor devices and platforms for data collection, i.e. radars, satellites and unmanned aerial vehicles; electronic warfare systems (electronic reconnaissance and counter-electronic effects) such as specially equipped aircraft, ships or vehicles; a large number of sensors that are integrated on combat and non-combat platforms to collect the necessary data.

The characteristic of IoT for use in the armed forces is that it must be standardized and secure, can connect via wire, satellites, mobile network, radio connection etc. They use special servers, but also dedicated and public servers depending on the needs and apply modern methods of storing and analyzing large amounts of data using machine learning. Military IoT uses a large number of sensors to collect the largest possible range of data, these sensors, among others, can be: audio, video, biological, atomic, chemical, thermal, radar, laser, RF, infrared, electro-optical, geolocation, for performance measurement, RFID, energy etc. Devices and platforms on which IoT is used can be personal portable devices, vehicles, ships, aircraft, unmanned systems (air, land and water) and computing devices. The above includes almost the entire spectrum of modern military equipment currently in use.

Even devices belonging to the third (obsolete) generation of military equipment have been upgraded in the last ten years in such a way that they can be considered IoT. All of the above devices have their own purpose for which they are used. If we take this purpose as a criterion for division, IoT is divided into:

- Personal IoT – They include tactical communication and information platforms that enable horizontal (between soldiers) and vertical (through the chain of command) communication, as well as platforms that monitor a person's health parameters;
- IoT for situational awareness – They enable satellite navigation, digital maps, the position and layout of their own and enemy forces, monitoring activities and coordination and control on the battlefield. For command personnel, these IoTs provide a broad picture of the operation zone, which is formed by collecting data from subordinate platforms directly on the ground;
- IoT for fire control – They are used in all types of armed forces, primarily for artillery and anti-aircraft fire, for guided missiles on land assets, aircraft, ships etc. They enable fully autonomous capabilities for the use of firepower. It is reflected in the control of the fire system, tracking over 100 targets simultaneously, target selection and fire that is pinpoint accurate because IoT segments are integrated into the ammunition itself, i.e. in the missiles and artillery shells used today. For this purpose, unmanned aerial vehicles are also widely used, which have become an indispensable integrated part of the fire control system;
- Logistic IoT – They involve the use of IoT for logistics and transport capacities. They are used to monitor the status of stored assets, delivery requests and their transport. In addition to the above, they can monitor basic logistical parameters of importance on the battlefield. The use goes so far that it is even possible to monitor the use of fuel in military equipment and its availability at distribution points;
- The use of IoT for personnel training – A set of sensors implemented on military equipment enables an exercise in which the participants are fully monitored in real-time. Their activities are sublimated so that trainers have the opportunity to guide the trainees in their actions in real-time. An example of the use of IoT can be taken as the use of the MILES (Multiple Integrated Laser Engagement System). It simulates real infantry combat but uses lasers instead of ammunition. During the exercise, soldiers run out of ammunition, are hit by “bullet or artillery fire” and are thrown out of the vehicle (“wounded or eliminated”). In addition, trainers have an instant overview of the complete situation in an imaginary armed battle. (Zheng & Carter, 2015).

It may be particularly interesting to consider the currently on-going personal IoT and those that a soldier will use in armed combat shortly. Modern armed forces currently use personal IoT that is predominantly related to communication and is reflected in a networked multifunctional horizontal and vertical connection with other participants in armed combat. Soon, personal IoT is expected to be used in communication (similar to now); situational awareness (tactical multifunctional mobile devices with a large number of additional sensors); medical surveillance (a platform that monitors vital health parameters and diagnoses); electronic warfare (electronic signal jamming devices) and independent power supply of all devices that are expected to be used by a soldier in the future (Fraga-Lamas, 2016).

6. Strategic and normative framework

For law, cyberspace represents a new, very dynamic and still incompletely regulated place in which perhaps too rapid changes are taking place, for which the legal order of a society or international organization does not always have an immediate and adequate response. This arises because the law itself represents a set of norms according to which an individual or community should function over a longer period. All norms codified in normative acts shape the legal system that, through public authorities, regulates all aspects of the functioning of the individual and society in general. Unlike law, cyberspace has not been limited by physical boundaries since its inception, and its technological side has enabled rapid changes and evolution of the form and method of functioning (Putnik, 2022).

This situation has forced societies and organizations to actively create and adapt strategic and normative frameworks to changes in cyberspace. Due to the complexity and development of cyberspace, modern societies recognize the need to establish international standards and norms that, following their specificities, would be transferred to the national level. However, establishing these standards, as well as applying existing ones at a time when cyberspace has become very topical and with a large number of states and entities that can exploit it, represents a serious challenge. The securitization of cyberspace is a current international topic with different views on it. Some countries, led by the USA, advocate the application of existing international norms, while others, such as the Russian Federation, emphasize the need to harmonize separate international agreements that would regulate this area.

The absence of a specific and clear source of international law leaves the possibility for countries to independently decide whether, for example, some cyber activity in cyberspace is equated with a kinetic armed attack. In general, taking into account the UN Charter and relevant UN resolutions, it has become an acceptable opinion that cyber operations whose effects are reflected in the destruction or incapacitation of human or material factors of the enemy party can be considered the use of force in international relations, regardless of the weapon used, because they produce the same effects as classical kinetic weapons. However, the question arises as to what to do with those cyber activities that do not do the above, but still have serious consequences for the functioning of society. In addition, it must be further considered that according to UN principles, it is acceptable to use classical armed self-defence only if there is an armed attack on the country.

Due to the existence of a legal vacuum, and the impossibility of fully applying the principle of legal succession, because cyberspace and activities in it differ from the starting principles in international law, i.e. the postulates of the UN, various initiatives have emerged that have addressed this issue. One of the most significant is the NATO initiative, which, over a long period, has brought together interested, prominent experts from several countries who are engaged in studying and organizing the most important facts when it comes to the use of the principles of international law in cyber warfare. So far, this initiative has resulted in the publication of manuals known as the first and second Tallinn Manuals (published in 2013 and 2017 by the University of Cambridge, while the third is currently under development as of 2021). Although they do not represent a legally binding interpretation, they reflect the positions of the authorities of the countries that initiated their publication (primarily NATO countries). Thus, the first manual opens up the possibility of self-defence with kinetic weapons if a cyber attack causes the destruction or incapacitation of the country's human and material factors. The second includes even more broadly the areas that

may be affected by cyber activities and establish positions and guidelines for potential action.

At the national level, the success of regulating cyberspace is defined by high-quality inter-sectoral cooperation and a complementary approach to defining norms related to cyberspace. This is achieved through documents such as, in the case of the Republic of Serbia, the Strategy for the Development of the Information Society and Information Security. The general goal of this strategy is, among other things, a developed information society and information security of citizens, public administration and the economy (Strategy for the Development of the Information Society and Information Security in the Republic of Serbia for the Period from 2021 to 2026, 2021). When it comes to the country's defence, the National Security Strategy and the Defence Strategy of the Republic of Serbia are of particular importance. of Serbia, which were adopted in 2019 and which only then, unlike the previous ones from 2009, recognize cyberspace, cyber security and cyber defence as factors influencing the overall security and defence of the country.

The National Security Strategy, when defining the issues of the strategic environment, recognizes that cyber threats can endanger the security of cyberspace through cyber espionage, attacks on critical infrastructure, unauthorized penetration of secret databases, as well as the spread of fake news and disinformation, while the part related to national security policy states that, when it comes to cyber security, it is stated that the ability and capacity to process, transfer and protect information and information and communication systems and defence against hybrid and information warfare techniques in information and cyberspace should continue to be improved. It is also stated that significant attention will be paid to the development of a general security culture of all citizens (National Security Strategy of the Republic of Serbia, 2019).

The Defence Strategy recognizes cyber-attacks as part of the factors that negatively affect the security environment through attacks on critical infrastructure facilities and the spread of fake news and disinformation within the concept of hybrid and information warfare. When it comes to challenges, risks and threats, it is stated that cyber-attacks on critical infrastructure facilities, high-tech crime, endangerment of information and communication systems, as well as the spread of fake news and disinformation within the concept of hybrid and information warfare, can negatively affect the functioning of elements of the defence system. Therefore, it is necessary to continuously develop technological and information protection of elements of the defence system at all levels of the organization. In the part related to defence policy and protection of the security of the state and citizens, the need to improve cybersecurity is recognized through improving the capabilities and capacities for coordinating work aimed at achieving cybersecurity and protecting against security risks in information and communication systems. The need to formulate a clear and coherent policy to increase the resilience of the aforementioned systems to incidents, to establish a network of competent entities for the fight against cyber actions and crime, as well as to improve cooperation between the public and private sectors in the field of cybersecurity is also recognized (Defence Strategy of the Republic of Serbia, 2019).

When, after the strategic framework, the normative framework is taken into consideration, it is important to first point out that it must, in addition to monitoring the development of cyberspace, also have a guiding role based on the prediction of the further development of that space in a particular society but also internationally. In the case of the Republic of Serbia, by assuming or accepting international obligations, the normative framework for cyberspace began to develop almost two decades ago by adopting laws and

enacting individual bylaws that elaborated the laws in more detail. At the very beginning, the Criminal Code and the Code of Criminal Procedure were amended, which defined the penalties and criminal procedure by which a criminal offence is established in cyberspace (Criminal Code, 2019) (Criminal Code, 2021).

Also, back in 2005, among other things, the law regulated the detection, prosecution and trial of criminal offences against the security of computer data as defined in the Criminal Code (Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime, 2023). The aforementioned law is constantly being adapted so that it experienced its last amendments in early 2023. After the above, when it comes to comprehensive cybersecurity, the Law on the Security and Information Agency and the Law on the Military Security and Military Intelligence Agency are characteristic. The former, in certain cases, allows, with the consent of the court, secret surveillance and recording of communications regardless of the form and technical means used, as well as static electronic surveillance of communications and information systems (Law on the Security and Information Agency, 2018). The second one regulates that the Military Security Agency implements measures to preserve the security of assets, data, industry, information and communication systems and cryptographic protection, as well as to detect and investigate acts that threaten classified data and the security of computer data. It also regulates that the Military Intelligence Agency may acquire, develop and use information systems and data transmission systems, as well as means of protecting information (Law on the Military Security and Military Intelligence Agency, 2013). Following these laws, laws dealing with data protection were successively adopted in the Republic of Serbia. These laws regulated the collection, processing and protection of personal data, information of public importance, secret data, business and professional secrets (Law on the Protection of Personal Data, 2018) (Law on the Protection of Business Secrets, 2021). In parallel with these laws, due to the expanding use of ICT, the Law on Electronic Communications was adopted, which comprehensively regulated electronic communications and electronic communications networks, and in a certain way regulated their security with the associated characteristics and priorities of the use of information networks for security and defence purposes (Law on Electronic Communications, 2023).

Following the above regulations, as a result of the further expansion of the use of cyberspace and the importance of the actions taking place in it, the obligation and need to adopt the Law on Information Security (first adopted in 2016, with the latest amendments and supplements in 2019) became mandatory. The above regulation establishes a system for the detection and prevention of cyber-attacks, defines the obligations, powers and coordination of existing and new entities (created by the adoption of the law) in cyberspace and in the event of cyber-attacks. The law establishes the basic principles of the protection of information and communication systems (risk management, comprehensiveness, as well as awareness and capability). Systems of particular importance are defined, which to a certain extent coincide with the factors of armed conflict, primarily when it comes to human and material resources, but also time, space and information. The National Centre for the Prevention of Security Risks in Information and Communication Systems (better known as the National CERT) has been established, as well as centers of government bodies and independent system operators with their respective areas of competence. The system for the functioning of cryptosecurity and protection against compromising electromagnetic radiation has been completed (Information Security Act, 2019).

Despite the progress made so far in the aforementioned strategies and laws, this progress is not sufficient in itself; rather, for the sake of a comprehensive and clear state response to contemporary challenges, risks and threats, it is necessary to adopt, following the example of most modern societies, an adequate national cybersecurity strategy and a national cyber defence strategy, which would be accompanied by additional legal solutions. The adoption of the aforementioned strategies and laws would be a prerequisite for creating an adequate legal framework for cybersecurity that includes "regulations regulating the responsibilities of authorities for managing security risks in information and communication systems and suppressing actions that threaten or disrupt the functioning of these systems, as well as norms on protection techniques, methods and procedures, coordination between protection actors, their responsibility and supervision over the implementation of legal powers and obligations" (Milošević & Putnik, 2017, p. 180).

To develop a comprehensive and complete strategic or legal framework for cybersecurity, it is necessary to understand and understand the principles of cyber warfare. The first eight principles were defined by Parks and Duggan at the beginning of the 21st century (Parks & Duggan, 2001). They are: (1) Cyber warfare must have concrete effects in the real world; (2) One party may take active steps to hide in the cyber world, but everything someone does is visible, the only question is whether anyone is watching; (3) There is no unchanging behaviour in cyberspace, except for that which requires action in the physical world; (4) Some entities in the cyber world have authorization to enter or perform any action that the attacker wants to be performed. The attacker's goal is to take the identity of these entities; (5) Cyber warfare tools have a dual role; (6) Attackers and defenders control a very small portion of the cyberspace they use. Whoever controls the portion of cyberspace used by an adversary can control the adversary; (7) Cyberspace is inconsistent and unreliable; (8) Physical constraints such as distance and space are not applicable in cyberspace.

Finally, the ninth principle, which emerged in the past decade, is defined by Putnik and Milošević as follows: “The assessment of security risks and threats in cyberspace is based primarily on the exponential law, while in the physical world it is based on the law of normal distribution” (Putnik, Milošević, & Bošković, 2017, p. 181).

One’s own military power, as well as that of the opponent, is traditionally viewed through the factors of armed combat. Often, these factors are easily measurable and comparable in armed conflict (number and training of personnel, types and number of military equipment, “depth of territory”, infrastructure etc.). However, with the emergence of cyberspace and the shaping of the principles of cyber warfare, the initial assumptions about one’s own and the enemy’s capacities are being questioned. The aforementioned principles of cyber warfare today change the perspective of armed combat factors in such a way that their importance is quite easily changed, or reduced.

Adopting appropriate strategies and further regulating the normative framework of cyberspace requires a different methodology than that applicable in the physical world. “Cyberspace is a realm of extreme events. Strategies that are considered good in physical warfare may be ineffective, even dangerous, in cyberspace. Entities in cyberspace behave significantly differently from what military experts are used to. It is almost certain that most entities within cyberspace, such as the physical and organizational topology of the network, undergo changes, most often in accordance with the exponential law. All activities that are carried out with the aim of carrying out attacks in cyberspace and causing damage to the adversary are also subject to this law. An adequate cyberspace defence policy should properly anticipate the challenges of exponential distribution, but also fully respect other

principles of cyber warfare, which undoubtedly question traditional principles of defence planning, both from an organizational and economic perspective." (Putnik, Milošević, & Bošković, 2017, p. 183).

The normative framework, developed on the above-mentioned principles, will enable the development of comprehensive resilience and protection of the factors of the armed struggle of a society in cyberspace. It will also have elements of prediction and successful guidance for the further development of cyberspace. In addition, it will contribute to raising awareness, knowledge and security culture in the broadest sense of the word, regardless of whether it is an ordinary citizen, a public institution, a private company or a scientific institute.

7. Conclusion

The general acceleration of processes in modern societies enabled by cyberspace and the development of ICT has brought a still unimaginable leap forward in overall progress. With it, the processes that bring about conflicts have also accelerated. Modern conflicts have changed their physiognomy compared to the conflicts that marked the 20th century, however, the goals for which they are fought have remained the same. Modern conflicts, although shorter, have become more comprehensive because they include all aspects of a society participating in an armed conflict. The factors of armed conflict represent everything decisive that a society can include in an armed conflict. Modern conflicts are also characterized by greater interconnectedness and mutual influence of the factors of armed conflict. Cyberspace, as a new circumstance, in the context of the history of armed conflicts, has brought about major changes, that is, its influence on the factors of armed conflict.

Each of the factors of armed conflict in the last few decades, due to the emergence of cyberspace, has begun to change almost completely, and the mutual influence has become such that the factors have become intertwined and dependent on each other. Cyberspace is still something new for some armed forces, for some, it is largely a part of space as a factor of armed conflict, while for a certain number of armed forces cyberspace has taken shape and can be considered a separate factor of armed conflict. It is unnecessary to talk about the connection and dependence of the human factor on cyberspace when every person is "online". The same can also be said for information. Material resources are currently characterized by the greatest changes, because in addition to technological progress, ICT with all its features are being implemented in. For modern armed forces, material resources represent a connection between cyberspace and the physical world. Artificial intelligence capabilities, interconnected resources and the development of IoT have completely changed the capabilities of the armed forces. Cyberspace for the armed forces represents the potential for victory but also the danger of losing in an armed conflict. The legal framework and normative order in a society must keep pace with the development, opportunities and dangers of cyberspace. The above can be considered preventive action and a prerequisite for building resilience to the factors of armed conflict.

The coming decades will be challenging for modern armed forces because cyberspace will require a change in the factors of armed combat compared to today's. Completely different capacities and abilities will be required from people. Completely new means of warfare will be used, which will be almost entirely IoT. Material resources and the optimization of their use through new scientific achievements will have much greater importance for armed conflict. The availability and flow of information will take on a

completely different dimension. Time and space will lose the importance they had and still have, except for time as a determinant of the duration of activities because many processes will take place almost instantly, unlike today.

Due to its connection and influence on other factors of armed combat, cyberspace will take on the characteristics of a separate factor, which, according to its characteristics, will be the most important and decisive factor of armed combat shortly.

Funding: This research was funded by the Scientific–Professional Society for Disaster Risk Management, Belgrade (https://upravljanje-rizicima.com/, accessed on 24 September 2024), and the International Institute for Disaster Research (https://idr.edu.rs/, accessed on 24 September 2024), Belgrade, Serbia.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Acknowledgements: The authors acknowledge the use of Grammarly Premium and ChatGPT 4.0 in the process of translating and improving the clarity and quality of the English language in this manuscript. The AI tools were used to assist in language enhancement but were not involved in the development of the scientific content. The authors take full responsibility for the originality, validity, and integrity of the manuscript.

References

1. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. (2023). *"Službeni glasnik RS", br. 61 od 18. jula 2005, 104 od 16. decembra 2009, 10 od 9. februara 2023, 10 od 9. februara 2023 – dr. zakon*.
2. (2017, mart 17). Preuzeto Januar 15, 2023 sa www.ibm.com: https://www.ibm.com/topics/machine-learning
3. (2021, oktobar 21). Preuzeto januar 14, 2023 sa www.adsinc.com: https://www.adsinc.com/news/c4isr-vs-c5isr-what-is-the-difference
4. Abell, N. (2020, oktobar 2). Preuzeto januar 15, 2023 sa https://medium.com: https://medium.com/@nqabell89/7-key-military-applications-of-machine-learning-9818dfa2ea86
5. Cintiriz, H., Buhur, M. N., & Sensoy, E. (2015). Military Implications of Big Data. *Proceedings of the International Conference on Military and Security Studies 2015* (str. 55-60). Istanbul: Turkish Army War College.
6. Cyberspace Operations. (2018, jun 8). Preuzeto januar 13, 2023 sa https://irp.fas.org/doddir/dod/jp3_12.pdf
7. Fraga-Lamas, P. F.-C.-A.-L. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors, 10*. doi:https://doi.org/10.3390/s16101644
8. Galan, J. J., Carrasco, R. A., & LaTorre, A. (2022, april 22). Military Applications of Machine Learning: A Bibliometric Perspective. *Mathematics, 10*.
9. George, G., Haas, M., & Pentland, A. S. (2014). Big Data And Management. *Academy of Management Journal*, 321-326.
10. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of The Hybrid Wars.* Arlington: Potomac Institute for Policy Studies.
11. *Hybrid Warfare: A New Phenomenon in Europe's Security Environment.* (2016). Prague: Jagello 2000 for NATO Information Centre in Prague.
12. *Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms.* (2016). Washington, D.C.: Joint Chiefs of Staf.
13. Lind, W. S., & Thiele, G. A. (2015). *4th Generation Warfare Handbook.* Kouvola, Finland: Castalia House.
14. National Security Strategy. (2022, oktobar 12). Preuzeto decembar 15, 2022 sa whitehouse.gov: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
15. North Atlantic Treaty Organization. (2022, mart 23). Preuzeto decembar 25, 2022 sa https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en
16. Parks, R. C., & Duggan, D. P. (2001). Principles of Cyber-warfare. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 122-125.
17. Putnik, N., & Milošević, M. (2018). Trends in Peace Research - Can Cyber Detente Lead to Lasting Peace. U B. Cook (Ur.), *Handbook of Research on Examining Global Peacemaking in the Digital age* (str. 1-19). Hershey: IGI Global.
18. Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., & Winkler, R. (2016). Analyzing the applicability of internet of things to the battlefield environment. *2016 international conference on military communications and*

information systems (ICMCIS), (pp. 1-8). Brussels. doi:10.1109/ICMCIS.2016.7496574
19. Zheng, D. E., & Carter, W. A. (2015). *Leveraging the Internet of Things for a More Efficient and Effective Military*. Washington, DC: Center for Strategic and International Studies.
20. Vojska Srbije. (2010). Preuzeto decembar 10, 2022 sa https://www.scribd.com/doc/270209153/Doktrina-Vojske-Srbije-kraj
21. Vojska Srbije. (2022). Preuzeto januar 10, 2023 sa https://www.vs.rs/sr_cyr/medjunarodna-saradnja/partnerstvo-za-mir/koncept-operativnih-sposobnosti
22. Zakon o Bezbednosno-informativnoj agenciji. (2018). *„Službeni glasnik RS", br. 42 od 19. jula 2002, 111 od 29. decembra 2009, 65 od 27. juna 2014 - US, 66 od 29. juna 2014, 36 od 10. maja 2018.*
23. Zakon o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji. (2013). *„Službeni glasnik RS", br. 88 od 28. oktobra 2009, 55 od 1. juna 2012 - US, 17 od 21. februara 2013.*
24. Zakon o elektronskim komunikacijama . (2023). *"Službeni glasnik RS", broj 35 od 29. aprila 2023.*
25. Zakon o zaštiti podataka o ličnosti. (2018). *"Službeni glasnik RS", broj 87 od 13. novembra 2018.*
26. Zakon o zaštiti poslovne tajne. (2021). *"Službeni glasnik RS", broj 53 od 28. maja 2021.*
27. Zakon o informacionoj bezbednosti. (2019). *Službeni glasnik RS br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019.*
28. Zakon o informacionoj bezbednosti. (2019). *"Službeni glasnik RS", br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019.*
29. Zakonik o krivičnom postupku. (2021). *"Službeni glasnik RS", br. 72 od 28. septembra 2011, 101 od 30. decembra 2011, 121 od 24. decembra 2012, 32 od 8. aprila 2013, 45 od 22. maja 2013, 55 od 23. maja 2014, 35 od 21. maja 2019, 27 od 24. marta 2021 - US, 62 od 17. juna 2021 - US.*
30. Krivični zakonik. (2019). *"Službeni glasnik RS", br. 85 od 6. oktobra 2005, 88 od 14. oktobra 2005 - ispravka, 107 od 2. decembra 2005 - ispravka, 72 od 3. septembra 2009, 111 od 29. decembra 2009, 121 od 24. decembra 2012, 104 od 27. novembra 2013, 108 od 10. oktobra 2014, 94 od* .
31. Milošević, M., & Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji–strateški i pravni okvir. *Kultura polisa*, 177-191.
32. Putnik, N. (2022). *Sajber rat i sajber mir*. Beograd: Univerzitet u Beogradu - Inovacioni centar Fakulteta bezbednosti.
33. Putnik, N., Milošević, M., & Bošković, M. (2017). Strateško planiranje sajber odbrane - ka adekvatnijem pravnom okviru i novoj koncepciji procene rizika, izazova i pretnji. *Vojno delo*, 174-185.
34. Strategija nacionalne bezbednosti Republike Srbije. (2019). *Službeni glasnik RS, broj 94 od 27. decembra 2019.*
35. Strategija odbrane R. Srbije. (2019). *Službeni glasnik RS, broj 94 od 27. decembra 2019.*

36. Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine. (2021). *Službeni glasnik RS broj 86 od 3. septembra 2021*.
37. Alemzadeh, M. (2023). Iran Protests and Patterns of State Repression. *Iranian Studies, 56*, 557-561. doi:10.1017/irn.2023.16
38. Babulak, E. (2010a). The 21st century cyberspace. *2010 IEEE 8th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 21-24. doi:10.1109/SAMI.2010.5423748
39. Babulak, E. (2010b). Keynote Speaker 3. doi:10.1109/AMS.2010.12
40. Bandura, A. (1999). Moral Disengagement in the Perpetration of Inhumanities. *Personality and Social Psychology Review, 3*, 193-209. doi:10.1207/s15327957pspr0303_3
41. Bogdanoski, M., & Milkovski, N. (2015). Information as a strategic resource critical to military operations and defence of the nation. Retrieved from https://consensus.app/papers/information-as-a-strategic-resource-critical-to-military-bogdanoski-milkovski/4a4330f794065928911ab7d9a5448944/
42. Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*. doi:10.1093/chinesejil/jmae005
43. Chkhikvishvili, G., & Beridze, S. (2024). Technological Progress in International Armed Conflicts. *Works of Georgian Technical University*. doi:10.36073/1512-0996-2024-2-294-300
44. Creveld, M. (1992). High technology and the transformation of war part II. *RUSI Journal, 137*, 61-64. doi:10.1080/03071849208445662
45. Cvetković, V. (2024a). Disaster Resilience: Guide for Prevention, Response and Recovery. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
46. Cvetković, V. (2024b). Disaster Risk Management. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
47. Cvetković, V. M., & Šišović, V. (2024). Community Disaster Resilience in Serbia. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
48. Cyberspace Operations. (2018).
49. Dexia, W. (2012). On the Effect of Scientific and Technological Progress and Its Applications in the Various Factors of Military Transformation. Retrieved from https://consensus.app/papers/on-the-effect-of-scientific-and-technological-progress-and-dexia/58a435cfd842534ea7ad52fb1d5ed5ca/
50. Dobash, R., Dobash, R., Cavanagh, K., & Lewis, R. (1996). Changing Violent Men. *Probation Journal, 43*, 217-218. doi:10.1177/026455059604300409
51. Friedmann, G. (1952). Technological Change and Human Relations. *British Journal of Sociology, 3*, 95. doi:10.2307/587488
52. Gareev, G. (2001). Problems of maintaining defense security in today's world. *European Security, 10*, 34-44. doi:10.1080/09662830108407503
53. Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security, 43*, 141-189. doi:10.1162/isec_a_00337
54. Grozdanić, G., & Cvetković, M. V. (2024). Exploring Multifaceted Factors Influencing Community Resilience to Earthquake-Induced Geohazards: Insights

from Montenegro. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
55. Hall, W. (2018). The Power of Will in International Conflict. doi:10.5040/9798400699825
56. Herolf, G. (1988). New technology favors defense. *Bulletin of The Atomic Scientists, 44*, 42-44. doi:10.1080/00963402.1988.11456200
57. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of The Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
58. Howe, J. (2006). Technology strategy and innovation in the defence context. 51-54. doi:10.1049/IC:20060225
59. Hubert, P. (2017). Déflagrant Délit. *Leonardo, 30*, 78-80. Retrieved from https://consensus.app/papers/d%C3%A9flagrant-d%C3%A9lit-hubert/2af0092ec4b65fe2a11a22df9b8439b5/
60. *Hybrid Warfare: A New Phenomenon in Europe's Security Environment*. (2016). Prague: Jagello 2000 for NATO Information Centre in Prague.
61. Johnson, J., Davis, R., Wester, R., Exner, F., Cowan, C., Patel, M., . . . Nachenberg, C. (1997). The military impact of information technology. *Communications of The ACM, 40*, 20-22. doi:10.1145/248448.248453
62. *Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms*. (2016). Washington, D.C.: Joint Chiefs of Staf.
63. Kellerman, A. (2010). Mobile Broadband Services and the Availability of Instant Access to Cyberspace. *Environment and Planning A, 42*, 2990-3005. doi:10.1068/a43283
64. Kier, E. (1995). Culture and Military Doctrine: France between the Wars. *International Security, 19*, 65-93. doi:10.2307/2539120
65. Kolganov, A. (2022). Fundamental civilizational shifts from the point of view of the method of political economy. *Noonomy and Noosociety. Almanac of Scientific Works of the S.Y. Witte INID*. doi:10.37930/2782-618x-2022-1-3-93-105
66. Kristoferson, L. (1981). Modern Weapons and the Environment. *Environmental Conservation, 8*, 257-258. doi:10.1017/S0376892900027909
67. Kupchyn, A., Dykhanovskyi, V., & Kolotukhin, Y. (2020). The war of the future as a strategic guideline for the forming the critical technologies list. *Journal of Scientific Papers "Social development and Security"*. doi:10.33445/sds.2020.10.1.2
68. Lan, T. (2021). Community of Common Future in Cyberspace. *The Oxford Handbook of Cyber Security*. doi:10.1093/oxfordhb/9780198800682.013.40
69. Libicki, M., Gompert, D., Frelinger, D., & Smith, R. (2007). Byting Back-Regaining Information Superiority Against 21st-Century Insurgents. Retrieved from https://consensus.app/papers/byting-backregaining-information-superiority-against-libicki-gompert/3f0c43f0090157debf049efb805ac3dd/
70. López, A. (2020). Necropolitics in the "Compassionate" City: Care/Brutality in San Francisco. *Medical Anthropology, 39*, 751-764. doi:10.1080/01459740.2020.1753046
71. Mbanaso, P., & Dandaura, P. E. S. (2015). The Cyberspace: Redefining A New World. Retrieved from https://consensus.app/papers/the-cyberspace-redefining-a-new-world-mbanaso-dandaura/12d1701141b65fe38975b33312fd62ab/
72. Milenković, D., Cvetković, V., & Renner, R. (2024). A Systematic Literary Review on Community Resilience Indicators: Adaptation and Application of the BRIC Method for Measuring Disasters Resilience. *Preprints*, 2024102277.

73. Milinovic, M., & Ivaniš, Ž. (2015). Advanced military concepts and organizations determined by technology requirements. 429-450. doi:10.2298/zmsdn1552429m
74. Muller, L. (2015). Cyber Security Capacity Building in Developing Countries. Retrieved from https://consensus.app/papers/cyber-security-capacity-building-in-developing-countries-muller/4e1728e1f9ee518b8d2663fea59c3248/
75. Neculcea, C.-A. (2021a). Information Operations. The Adequate Communication Response to Contemporary Threats. *Romanian Military Thinking*. doi:10.55535/rmt.2021.4.05
76. Neculcea, C.-A. (2021b). Operaţiile informaţionale – răspunsul comunicaţional adecvat la ameninţările contemporane. *Gândirea Militară Românească*. doi:10.55535/gmr.2021.4.05
77. Pysarenko, T., Kvasha, T., Bohomazova, V., Paladchenko, O., Molchanova, I., & Shabranska, N. (2024). Defense-industrial complex: scientific and technological trends. doi:10.35668/978-966-479-140-0
78. Reese. (2020). Operations in the Information Environment Application of the direct and indirect approach for by LtCol C. Retrieved from https://consensus.app/papers/operations-in-the-information-environment-application-of-reese/473f67141c1c596d9dceccd2a046461e/
79. Santala, R. (2004). Don't Start the Revolution Without Me: A Review of the Army Transformation. Retrieved from https://consensus.app/papers/dont-start-the-revolution-without-me-a-review-of-the-army-santala/5a46ed75c23a580a81e2a754ec9741c5/
80. Schinkel, W. (2004). The Will to Violence. *Theoretical Criminology, 8*, 31-35. doi:10.1177/1362480604039739
81. Serrano, Y., & López, W. (2008). Estrategias de comunicación militar y dinámicas mediáticas ¿dos lógicas contradictorias? , *4*, 269-277. doi:10.15332/S1794-9998.2008.0002.04
82. Sim, S. (2023). The Development of Digital Technologies and Cyber Security Threats. *Sungshin Women's University Center for East Asian Studies*. doi:10.56022/ceas.2023.29.1.197
83. Stepanyants, M. (2022). Problems of Civilizational Development in the Leading Countries of the Asian Region. *Voprosy Filosofii*. doi:10.21146/0042-8744-2022-7-5-14
84. Tanasić, J., & Cvetković, V. (2024). The Efficiency of Disaster and Crisis Management Policy at the Local Level: Lessons from Serbia. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
85. Toroi, G.-I. (2021). Information activities – essential warfighting function in today's military operations. Retrieved from https://consensus.app/papers/information-activities-%E2%80%93-essential-warfighting-function/86c0c34fb67552999a305200b7fd80df/
86. Townsend, T., Dillard-Wright, J., Prestwich, K., Alapatt, V.-A., Kouame, G., Kubicki, J., . . . Williams, C. (2023). Public safety redefined: Mitigating trauma by centering the community in community mental health. *The American psychologist, 78 2*, 227-243. doi:10.1037/amp0001081
87. Urbatsch, R. (2021). Physical formidability and acceptance of police violence. *Evolution and Human Behavior*. doi:10.1016/J.EVOLHUMBEHAV.2021.03.008

88. Van Swol, L., Prahl, A., MacGeorge, E., & Branch, S. (2019). Imposing Advice on Powerful People. *Communication Reports, 32*, 173-187. doi:10.1080/08934215.2019.1655082
89. Westing, A. (1988). The Military Sector vis-à-vis the Environment. *Journal of Peace Research, 25*, 257-264. doi:10.1177/002234338802500305
90. Wilén, N., & Strömbom, L. (2021). A versatile organisation: Mapping the military's core roles in a changing security environment. *European Journal of International Security, 7*, 18-37. doi:10.1017/eis.2021.27
91. Zgirovskaya, E. V. (2023). Providing scientific and technological progress as a function of the modern state. *Proceedings of the 6th International Conference "Futurity designing. Digital reality problems"*. doi:10.20948/future-2023-12
92. Ноономика, Б. С. Д., Альманах, Н., С.Ю, И. И., Том, В., Бодрунов, С. Д., Нооообщество, Н., 新兴工业发展研究所, 俄罗斯圣彼得堡, 博. (2022). Scientific and technological progress and transformation of society: noonomy and noosociety. Part 1. *Noonomy and Noosociety. Almanac of Scientific Works of the S.Y. Witte INID*. doi:10.37930/2782-618x-2022-1-1-24-42
93. Putnik, N. (2022). *Sajber rat i sajber mir*. Beograd: Univerzitet u Beogradu - Inovacioni centar Fakulteta bezbednosti.

UDK: 343.9.02:004.7

ORGANIZED CYBER CRIME: ADVANCING INVESTIGATIONS OF CRIMINAL ONLINE ACTIVITIES AS A POTENTIAL FORM OF ORGANIZED CRIME

Aleksandar Pešev
MA Faculty of Security – Skopje
aleksandar.peshev78@uklo.edu.mk

Abstract

Suggesting that cyber-crime is a novel modern-day threat may seem like a tired and worn expression that held its relevance at the dawn of the twenty first century. Police forces globally have addressed this form of crime with the formation of separate departments for tackling cybercrime and their success is evident with arrests of black hat hackers and cyber criminals. Unsubs are often profiled as loners aiming to provide proof of skills for personal gratification or aspiring criminals seeking to make easy money. But what happens when the stereotypical "kid in a hoodie hacking from a childhood bedroom" joins forces with others in achieving a set goal. This often leads to another stereotypical interpretation: activists joining forces for a defined cause, or hacktivism. But what if the intent is criminal? What if the members of the group are tasked with specific roles in hierarchical fashion with set tasks, and the criminal activity traverses the cyber realm and the real world? This poses challenges for police forces in addressing a new form of organized crime that primarily exploits computer systems, causing real life consequences, not only to individual users but to organizations and governments.

Keywords: Organized crime, Cyber-crime, Organized Cyber Crime, Police.

Introduction

Technological advancements clearly advance new forms of crime, posing new and unique challenges for police and law enforcement agencies. Initially considered as the malevolent hobby for a select group of advanced computer users, modern cybercrime has become more accessible and easier to execute. With no need for expensive equipment, nor special skills, this type of crime is showing signs of evolving into a separate form of organized crime. What sets organized cyber-crime apart from hacking and so-called "traditional" cybercrime is the component of organization, with strict roles for each of the individuals involved, and indications of a hierarchy in the modus operandi. Compared to a few people skimming credit card numbers at local ATMs, the criminal activities of an organized cybercrime group pose a much broader threat to security. Apart from endangering the safety and wellbeing of select victims, organized cybercrime poses a threat to the security of private entities, as well as state institutions.

In turn, this poses a unique challenge for the police. While cybercrime is hardly a novel occurrence in the criminal world, the evolution of cybercrime into a more organized form warrants an enhanced cooperation between the cybercrime and organized crime departments, which are traditionally segregated within the police force. The formation of special task forces or hybrid departments is also an option, depending on the frequency of

criminal activity conducted with the aid of the Internet. As a case study will demonstrate, some of these criminal activities often cross over from the computer screens into the real world, with the use of money mules and covert transactions, involving suspected collaborators within organizations. The severity of this issue is underlined by the estimate that the annual damages from cybercrime amount from 445 to 600 billion US dollars.

Popular culture may portray the black hat hacker as a loner, aiming to infiltrate a closed system for fun or profit. The emergence of structure in these activities with strictly defined roles and duties of the criminals involved, suggests an evolution which signals two major security risks. The first is the risk of shifting traditional organized crime to the cyber realm, actively exploiting the talent of hackers, from script kiddies to advanced coders. Some of this talent is readily available to purchase as ready to use products on the dark web, from malicious code to black hat hackers for hire. The second indicated security risk is the potential evolution of a new breed of organized crime: one that does not require real world contacts, physical threats or face-to-face extortion. All that is needed (for a start, at least) is some skill and a stable internet connection.

Defining cybercrime

In order to form the basis for providing a working definition of organized cybercrime, a definition for cybercrime as the core itself is warranted. While organized cybercrime is evolving into a separate type of criminal activity, it is challenging to form a comprehensive definition of cybercrime that is acceptable for police forces across nations. A common approach is to define it in two categories: cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes are crimes that can only be committed by using Information and Communication Technologies (ICTs). A notorious example is ransomware: hacking into an organization or individual's device, encrypting data and demanding payment for decryption. Cyber-enabled crimes are so-called traditional crimes that have been transformed in speed, scale and scope through the use of ICTs, such as online banking scams, identity theft or fraud, and online child sexual exploitation (Wilkinson, n.d.). To make the distinction even more evident, the following differences may be underlined:

- Cyber-dependent crimes require ICTs for the criminal act to be executed. Without a network, commonly the Internet, these crimes would not be possible.
- Cyber-enabled crimes commence in the real world and utilize computers and networks to facilitate the criminal activity. Criminal acts like the unauthorized sale/dealing of narcotic substances may be conducted on illicit internet sites. The sale of narcotics in and of itself is possible without the Internet but may be facilitated by taking the deals on-line.

This distinction answers the question of how a crime can be committed with the use of ICTs, leaving room for the additional components of criminalistic analysis: who performs the crime and who are the victims?

As to the question of who the criminals are, the categorization of hackers comes into consideration. Hackers engaging in criminal activity are dubbed as black hat hackers, with white hat hackers engaging in penetration testing and cyber security, on the other side of the frontline. Grey hat hackers is a term used to describe individuals who occasionally engage in illegal activity online in terms of gaining unauthorized access into a system or a network, who also work on the legal side with their activities (Димовски, 2016).

Defining the types of hackers completes one element of the criminalistic triangle, with the initial specification of the perpetrators. The means covers the second aspect, in reference to location. The third aspect is the target or the victims. This is where the organized crime

component comes into consideration. If a singular black hat or grey hat hacker attacks a number of individual users, the use of the term organized cybercrime is inapplicable. However, should a group of black hats, functioning in an organized manner attack a selected target, it may be noted that the crime in question is organized cybercrime. Further study of organized cybercrime is indeed warranted, and will be presented further on, however, in order to form a solid argument for this distinction, a more detailed overview of the historical elements of cybercrime is required.

Evolution of cybercrime

Cybercrime is dependent on the access to networked computer systems that store or exchange data that may be exploited in different illegal ways. The increased frequency of this criminal activity is corelated with the spread of the Internet, initially envisioned as a series of networked computers exchanging data. Paving the way for the information age was the Defence Advanced Research Projects Agency (DARPA, prev. ARPA). ARPA research played a central role in launching the Information Revolution. The agency developed and furthered much of the conceptual basis for the ARPANET—prototypical communications network launched nearly half a century ago—and invented the digital protocols that gave birth to the Internet. DARPA also provided many of the essential advances that made possible today's computers and communications systems, including seminal technological achievements that support the speech recognition, touch-screen displays, accelerometers, and wireless capabilities at the core of today's smartphones and tablets. DARPA has also long been a leader in the development of artificial intelligence, machine intelligence and semi-autonomous systems. DARPA's efforts in this domain have focused primarily on military operations, including command and control, but the commercial sector has adopted and expanded upon many of the agency's results to develop wide-spread applications in fields as diverse as manufacturing, entertainment and education (*78 DARPA 50 Years of Bridging the Gap*, n.d.).

Contributing to the concept of networked communication was the Paolo Alto Research Centre or PARC, within the US company Xerox. The centre is also credited for the Graphic User Interface (GUI), that inspired modern computer operating systems. (Severance, 2013).

The decision to take the ARPANET public was made in 1993, paving the way for the modern internet. Initially the network was envisioned as a technology that would advance the exchange of information between researchers and non-profit institutions. (Manros, 1998).

This short history overview is meant to lead to the point that from its inception, security was likely not a dominating concern for internet users, as the network in its earliest form was intended for scientific research and exchanges. Soon after going public, though, malicious activities followed. Initial information on hackers was a declared drive to gain access to something that was kept away from public knowledge, as even in the early stages, the Internet had a public segment (the .com) and a segment that was kept private, accessible to authorized users only.

The first recorded case of hacking into a computer network in the Internet era dated back to 1986 when Marcus Hess was charged for unauthorized collection of information from the Lorence Berkley national laboratory. According to the charges, Hess was allegedly selling collected data to the Soviet intelligence service, the KGB. It is relevant to note that authorities in Wester Berlin at the time arrested collaborators of the suspect, charged with mediating the transfer of the stolen information. Looking at this case, the following dilemma

is posed: The activity involved multiple people, with profits involved. While analysing the case based on the activities of the persons involved may lead to the conclusion that this is an early example of an organized crime group, the sale of information to the Soviet Union makes it a case for the intelligence and counterintelligence agencies, who also counter organized crime. So where do the police come in as the sole leader in a case against organized cybercrime? An early case that would warrant police forces to take the charge and lead the case against cybercrime is that of Vladimir Levin who in 1994 managed to steal 10 million US dollars from "City Bank", in collaboration with his associates. The heist involved acquiring usernames and passwords of the bank's employees (*The History of Computer Hacking*, n.d.).

Both cases seem to comply with the noted elements of organized crime, as outlined by Labovic and Nikolovski:

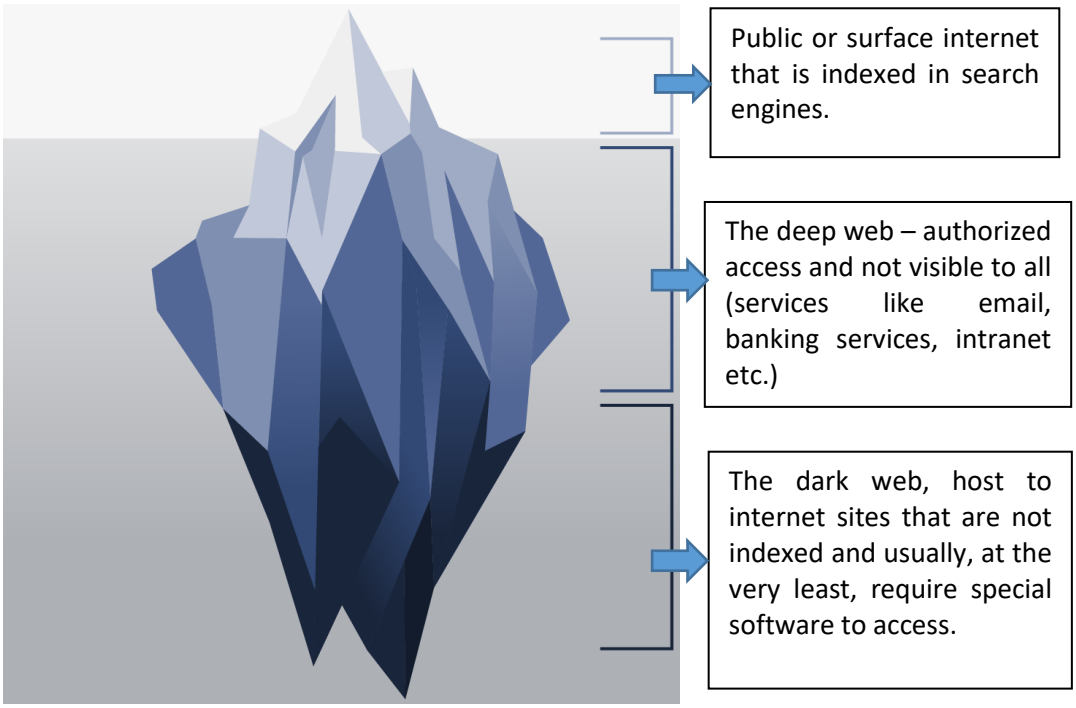
- Organized criminal action of at least three or more individuals for whom there is evidence of an agreement and specifications for their roles;
- Evidence claim that the criminal activities have been ongoing for a set period of time. This is especially evident in the first case that involved sale of information to the Soviet Union;
- Both cases resulted with criminal charges;
- In both cases the criminals made financial and material gains.

While both cases exhibit elements of organized crime that primarily instrumentalized the early Internet as means for making illegal profits, modern day cases are significantly more complex. An example is the now shut down Silk Road, which was an online black market known also as the first darknet market. It was launched in 2011 by Ross Ulbricht under the pseudonym "Dread Pirate Roberts and primarily sold illegal narcotics. This darknet market did not appear in a standard web search, but rather in the deeper parts of the Internet.

The iceberg beneath the public internet

As previously noted, in its early days the Internet had two basic levels: the public access domains, most commonly in the form of commercial sites, and the private part of the world wide web, with limited access for authorized users. The spread of the Internet, however, formed at least one major segment under the tip of the publicly visible tip of the iceberg: the dark web.

Illustration: The major levels of the Internet (from ehacking.net)



Providing this illustration may seem redundant, especially for tech-savvy users and experienced investigators who will likely immediately note that the majority of cybercrime either links to or occurs on the darknet. The aforementioned SilkRoad darksite set the president for this practice in the dealing of narcotics. The reason such an illustration is deemed as necessary is because of an additional characteristic of organized crime groups, as noted by Interpol: With revenues estimated in the billons, their criminal enterprises closely resemble those of legitimate international businesses (*Organized Crime*, n.d.).

It is in this context that a new security risk is potentially identified, posing an additional challenge for police investigators: Businesses of organized crime groups, posing as legitimate enterprises on the public web can hypothetically link to the dark web. This phenomenon of surfacing a legitimate site that is connecting to the dark web may likely be made in order to draw in potential collaborators, as well as potential victims. An additional point of connection between a public site and a dark web site may be the use of crypto currency as means of trade and compensation. This may pose an additional challenge to investigators as crypto currencies are difficult to trace.

Weather focused exclusively on the dark web or surfacing to the tip of the iceberg in the public internet, organized crime groups have several major areas for potential illicit profit.

The first category of criminal "services" is concerning offers of illegal substances, or criminal services. Aside from narcotics as mentioned above, additional services may and do involve:

- code or scripts for a ready-made cyber-attack (persons utilizing such attacks are known as script kiddies);
- Hackers (black hats) for hire
- Sale of illicit substances – narcotics or banned goods in certain countries
- Sale of weapons, ammunition and explosives

- Human trafficking
- Child pornography
- Sale of "services": mercenaries, assassinations, re-entering, extortion, theft
- Selling espionage services, weather cyber espionage or real-world spying

While this list is hardly extensive, and the offer is only limited by the imagination of the criminal mind, it is difficult to argue against the appeal that such opportunities would pose for organized crime groups.

Taking organized crime online

Building upon the initial distinction between Cyber-dependent crimes (needs a network to do the crime, which would be impossible without the Internet) and Cyber-enabled crimes (the network helps the execution of the criminal act), organized crime groups may see cybercrime as a potentially profitable criminal endeavour. This is noted in the Interpol Global Strategy on Organized and Emerging crimes, stating the following: Traditional structures headed by powerful kingpins controlling niche crimes are increasingly replaced by loose, flexible criminal networks that shift operations and modify their business models based on opportunities, incentives, profitability and demand. The ease of international trade and travel, instantaneous access to information, advanced technology and widespread encrypted communication provide ripe terrain for transnational crime to flourish (Interpol, 2017).

The noted rise in encrypted communication indicates the initial benefit that organized crime groups may have from the Internet. Though not intended for criminal activities, platforms for encrypted communications ease the activities of members of organized crime groups by making detection and signal intelligence efforts more difficult and in some cases completely untraceable. This indicates that encrypted communication is abused for large scale criminal activities, possibly crossing borders (transnational organized crime) that occur in the real world and not online. This, however, cannot remain as the sole challenge for police.

The second possibility is in regard to incorporating cybercrime within organized crime activities, in the form of cyber-enabled crimes. This would involve recruitment of black or grey hat hackers for the purposes of facilitating criminal activities on a larger scale, both within the borders of a nation, or internationally. Noteworthy is the hypothetical positioning of black hat hackers in this form of organized crime. It is likely that the black or grey hats would not be a permanent member of an organized crime group, if they offer their services for a fee on the dark web. If the criminal activity of the organized crime group is intended to last for an extended period of time, black hats would likely be recruited as members of the organized crime group. In theory, their skillset would be paramount, while their influence may be limited. Depending on the skills the black hat may possess (common skillset or specialized ability that is hard to come by), the hackers may become invaluable members of the group, or be easily replicable, hence expendable. A possible hypothesis would be that the level of trust that a black hat enjoys within an organized crime group is correlated to his or her usefulness in executing the crime.

The third security risk is identified in the formation of organized crime groups that function exclusively on-line, in line with the cyber-dependent crimes. The international component is often evident, and if an organizational structure is defined, lasting for a set period of time with significant profits from criminal activities, the case can be made for organized cybercrime. An organized cybercrime group would hypothetically fit the definition of organized crime, with their criminal activity being primarily cyber dependent.

This, however, does not necessarily mean that all criminal activity must and will be limited exclusively in the cyber domain.

Case study: The robbery of bangladesh bank

Presented as the largest cyber robbery of the XXI century (to date), the bank heist that took 80 million USD from the Bangladesh Central Bank contains elements that comply with existing definitions for organized crime. Judging from media reports, the robbery can be viewed as both cyber enabled and cyber dependent. Aspects of the crime that make it cyber dependent is the use of malware that exploited the vulnerabilities in the bank's computer system, as well as the system for international bank transfers known as SWIFT (*Malware Suspected in Bangladesh Bank Heist: Officials | Reuters*, n.d.). Some media reports suggest that suspected hackers gained unauthorized access to the system several times in the period from 24.01 to 06.02.2016, before the robbery was executed. The goal was to identify the vulnerabilities of the system, that enabled the spread of the malicious code. (*Hackers Stalked Bangladesh Bank for Two Weeks Before Big Heist - Bloomberg*, n.d.).

The following timeline of key events can be compiled using media reports:

- Hackers send email to bank computers containing the malware. A group from North Korea is noted as potential suspected organizer of the cyber-attack;
- Bank employee opens the message, containing malware disguised as a text document;
- The malware spreads on bank servers and steals usernames and passwords of employees;
- Attackers gain access to the SWIFT system, used for transfers between banks;
- Hackers use stolen credentials to submit 35 transfer requests to the Federal Reserve in New York, USA;
- Four transfer requests are approved amounting to over 80 million USD;
- Funds are transferred to four bank accounts in the Philippines in the RCBC bank;
- Four unidentified individuals empty the bank accounts in the Philippines and transfer the money to the PhilRem company. Philippine authorities manage to recover 15 million USD, while the rest of the money in laundered in casinos in Manilla.

The use of money mules can lead to the interpretation of this crime as a cyber-enabled one, though it is difficult to make this argument, as the crime would have not been possible in the first place if hackers did not manage to gain access to the SWIFT system in the Bank of Bangladesh. Until the year 2020 there is no publicly available information that suggest a resolution to this crime. (*Bangladesh Bank Cyber Heist: No Solution for Biggest Hacking*, n.d.).

The case, however, serves as a solid base for analysing international cyber-enabled organized crime with the use of ICTs, or organized cybercrime as the term used in this paper. The following definition for organized crime, as referenced by the Council of Europe, will be set as the basis for the analysis: Organized crime involves illegal activities undertaken by a structured group consisting of three or more persons, who collaborate over an extended period of time, for the purpose of conducting one or more serios crimes, for gaining financial, material or other gains (Лабовиќ & Николовски, 2010).

Should the case be viewed through the framework that this definition sets, the following analytical elements may be considered:

- There are indications that the cyber robbery of the Central Bank has been conducted by a group of three or more people. It is unknown if the group was structured or not, there is no indication from publicly available information. Claims from the American FBI, that the attack was conducted by a state entity, likely a group from North Korea may suggest some form of structure, as most entities in North Korea are under state control.
- In order to confirm if the organized criminal group has existed for a prolonged or longer period of time (aside from the unspecified duration in the definition – what is meant by "longer" or "extended period of time?) a final report on the robbery is necessary, resulting from an international investigation. The information that the group gained unauthorized access to the bank's systems on several occasions (Balu, n.d.) may attest to the longevity of the organized crime group that executed the heist.
- Common activity for investigating one or multiple crimes is evident from the case itself: unauthorized access, data theft, abuse of the SWIFT system, robbery and indicated money laundering.
- The seriousness of the crime is evident from the case itself.

Organized crime and organized cybercrime – similarities and differences

The presented information to this point suggests a number of similarities between organized crime and organized cybercrime. There is, however, one key question that is produced from the theoretical research: does a group of individuals formed for the purpose of a single cyber-attack qualify as an organized crime group? If this dilemma is addressed using the case study of the robbery of the Bangladesh Central Bank, it is evident that a group of petty criminals is not likely to steal 8 million USD, resulting in international doubts around the security of the system used by multiple banks for large transfers. With the criteria for seriousness of the crime being met, cyber criminals engaged in an organized activity for a set period of time resulting in serious damages meet the criteria to be defined as an organized criminal group. The only problematic element that distinguishes organized cybercrime from "traditional" organized crime is the longevity of the organization. As Thomas Holt states that while there are certainly some states that are involved in cybercrime, those who cause the most serious damage are individuals who gather together for the accomplishment of a singular goal and then disappear (*Organized Cybercrime—Not Your Average Mafia*, n.d.).

The basis for analysing the form of an organization and the ways of organizing are set by the model of Best and Luckenbill (Best & Luckenbill, 1981) aiming to make a distinction between the roles of the persons involved and their associations. The sociological model is presented in Table 1:

Table 1: Framework of social organization – Best and Luckenbill

Organizational form	***Characteristics***			
	Mutual acquaintance	Mutual participation	Elaborated division of labor	Expanded organization
Loners	×	×	×	×
Colleagues	✓	×	×	×
Peers	✓	✓	×	×
Teams	✓	✓	✓	×
Formal organizations	✓	✓	✓	✓

It is worth mentioning that the was that a criminal group organizes itself is largely conditioned by the time and location of the criminal act, as well as the laws and regulations that are applicable at the time of the deed. It may be considered that members of a criminal group may not need to have fixed roles, and their contributions may vary depending on conditions. Following the aforementioned model, if cybercrime is conducted by a loner, that it may be possible for one person to play multiple roles, from administering malware to visiting a bank location in order to empty accounts. However, this flexibility is likely to reduce if the crime is more sophisticated, as such an activity would warrant the involvement of multiple people. A high-profile crime would likely warrant the involvement of individuals with specialized skills, executing high-skill tasks.

In an attempt to address the issue of whether a group of hackers who group together on a part time basis for a singular criminal act qualifies as organized crime, Leukfeldt and Holt gathered information from 18 criminal investigations in the Netherlands concerning cybercrimes. The authors note that the majority of groups exhibit organizational complexity based on the division of labour as well as the extended time period of their existence (Leukfeldt & Holt, 2020). Following the model of Best and Luckenbill, the researchers note that from the analysed sample, the majority of the groups that were subject to investigation were classified ad “teams” or “formal organizations”. A total of 32 identified networks from this research fall within one of these two categories, leading to the potential conclusion that the criminal activity in question is organized crime.

CONCLUSION: CHALLENGES FOR POLICE

The paper has attempted to follow two forms of criminal activity, suggesting the formation of a hybrid between organized crime and cybercrime. In terms of hacking and illegal activities online, evolving challenges such as Artificial Intelligence create new potential for criminal activity. The potential for fabrication of credentials, fabrication of evidence, extortion and simplified creation of potentially malicious code are just some of the challenges stemming from generative AI alone. While these challenges require separate research, it would be unwise to ignore the possibility that organized crime groups could utilize this evolving technology for criminal purposes, weather in cyber-enabled or cyber-dependent criminal activities.

Organized crime is likely to evolve in the cyber realm weather as organized crime groups venturing into the cyber world or black hat hackers acting together as "old fashioned" organized crime groups in the real world. What does this mean for the police force? While police forces across nations have succeeded in addressing both of these forms of crime separately, with the formation of teams, task forces or departments tasked with investigating and building solid cases for further prosecution. Proactive measures are also evidenced on both fronts, in cybercrime and in organized crime. The challenge that is posed is evidenced by the merging of these two threats, effectively blurring the lines between organized crime in the real world and in cyberspace.

This poses the need for increased interdepartmental cooperation within police forces of individual nations, potential formation of task forces from both the organized crime and the cybercrime departments, as well as enhanced international cooperation on the subject of organized cybercrime.

REFERENCES

78 DARPA 50 Years of Bridging the Gap. (n.d.).

Balu, R. (n.d.). *Bangladesh Bank Cyber Heist: Incident Analysis*. Retrieved October 30, 2024, from www.swift.com

Bangladesh Bank cyber heist: No solution for biggest hacking. (n.d.). Retrieved April 14, 2021, from https://www.thedailystar.net/frontpage/bangladesh-bank-hacking-no-solution-biggest-cyber-heist-in-history-1863118

Best, J., & Luckenbill, D. F. (1981). Tender feet and high stepping: Soring in the Tennessee walking horse industry. *Deviant Behavior*, *2*(3), 231–259. https://doi.org/10.1080/01639625.1981.9967555

Hackers Stalked Bangladesh Bank for Two Weeks Before Big Heist - Bloomberg. (n.d.). Retrieved April 14, 2021, from https://www.bloomberg.com/news/articles/2016-03-18/hackers-stalked-bangladesh-bank-for-two-weeks-before-big-heist

Isabella Wilkinson. (2023, August 4). *What is the UN cybercrime treaty and why does it matter?* Https://Www.Chathamhouse.Org/2023/08/What-Un-Cybercrime-Treaty-and-Why-Does-It-Matter.

Leukfeldt, E. R., & Holt, T. J. (2020). Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522–538. https://doi.org/10.1177/0306624X19895886

Malware suspected in Bangladesh bank heist: officials | Reuters. (n.d.). Retrieved April 14, 2021, from https://www.reuters.com/article/us-usa-fed-bangladesh-malware-idUSKCN0WD1EV

Manros, C.-U. (1998). The birth of the Internet printing protocol (IPP). *StandardView*, *6*(4), 135–139. https://doi.org/10.1145/338183.338184

Organized crime. (n.d.). Retrieved October 30, 2024, from https://www.interpol.int/en/Crimes/Organized-crime

Organized cybercrime—not your average mafia. (n.d.). Retrieved March 14, 2021, from https://phys.org/news/2020-01-cybercrimenot-average-mafia.html

Severance, C. (2013). Bob metcalfe: Ethernet at forty. *Computer*, *46*(5), 6–9. https://doi.org/10.1109/MC.2013.159

The History of Computer Hacking. (n.d.). Retrieved April 12, 2021, from https://www.newsweek.com/history-computer-hacking-69449

Димовски, З. (2016). *Криминалистичко Разузнавање*. Факултет за Безбедност, Скопје.

Лабовиќ, М. (Факултет за Б.-С., & Николовски, М. (Факултет за Б.-С. (2010). *Организиран Криминал и Корупција* (Љ. Арнауговски & М. Ангелески, Eds.). Факултет за Безбедност, Скопје.