ICONO 14, Revista de comunicación y tecnologías emergentes
ISSN: 1697-8293
info@icono14.net
Asociación científica ICONO 14
España

Juurvee, Ivo; Arold, Uku

Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats

ICONO 14, Revista de comunicación y tecnologías emergentes, vol. 19, no. 1, 2021, -June, pp. 70-94
Asociación científica ICONO 14
España

DOI: https://doi.org/10.7195/ri14.v19i1.1628

Available in: https://www.redalyc.org/articulo.oa?id=552565288004

MONOGRAPH

Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats

Defensa psicológica y ciberseguridad: Dos aproximaciones del enfoque integral de Estonia para contrarrestar las amenazas híbridas

Defesa psicológica e segurança cibernética: Duas partes da abordagem abrangente da Estônia para combater ameaças híbridas

Dr. Ivo Juurvee
Head of Security & Resilience Programme
(International Centre for Defence and Security)
https://orcid.org/0000-0001-9239-047X
Estonia

Maj. Uku Arold
Lecturer of information conflicts
(Estonian Academy of Security Sciences and Estonian Military Academy)
https://orcid.org/0000-0002-6877-8957
Estonia

Reception date: 18 September 2020
Review date: 18 November 2020
Accepted date: 7 December 2020
Published: 1 January 2021
To cite this article: Juurvee, I. & Arold, U. (2021). Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats, *Icono 14, 19*(1), 70-94. doi: 10.7195/ri14.v19i1.1628

Abstract

Disruptive developments in the field of information and communication technology have enabled malicious actors to turn elements of the digital ecosystem into information weapons in hybrid conflict. Estonia has tackled the new security realm with comprehensive national defence that is built upon understanding that the society itself is object of security and should provide appropriate safeguards and responses. Estonian conceptualisations of national cybersecurity, psychological defence, and strategic communications are elaborated in the light of actual seminal threat situations. Analysis of evolvement of the strategic documents guides the recommendations for even deeper blend of the technical cybersecurity culture with value-centric psychological defence and internationalisation of information security situational awareness and planning.

Key Words: *Estonia; Russia; Hybrid threats; Cyber; Psychological defence; Strategic communications (stratcom); Information warfar;, Information environment; Cyberspace; Information weapon; Cyber weapon; Cybersecurity*

Resumen

Los avances disruptivos en el campo de la tecnología de la información y las comunicaciones han permitido a los actores malintencionados convertir elementos del ecosistema digital en armas de información en conflictos híbridos. Estonia ha abordado el nuevo ámbito de la seguridad con una defensa nacional integral que se basa en el entendimiento de que la propia sociedad es objeto de seguridad y debe proporcionar las salvaguardias y las respuestas adecuadas. Las conceptualizaciones estonias de la ciberseguridad nacional, la ciberdefensa psicológica y las comunicaciones estratégicas se elaboran a la luz de situaciones reales de amenazas seminales. El análisis de la evolución de los documentos estratégicos guía las recomendaciones para una combinación aún más profunda de la cultura técnica de ciberseguridad con la defensa psicológica centrada en el valor y la internacionalización de la planificación y el conocimiento de la situación de la seguridad de la información.

Palabras clave: *Estonia; Rusia; Amenazas híbridas; Cyber; Defensa psicológica; Comunicaciones estratégicas (stratcom); Warfar de información, entorno de información; Ciberespacio; Arma de información; Arma cibernética; La seguridad cibernética*

Resumo

Desenvolvimentos disruptivos no campo da tecnologia da informação e comunicação permitiram que atores maliciosos transformassem elementos do ecossistema digital em armas de informação em conflitos híbridos. A Estônia abordou o novo domínio da segurança com uma defesa nacional abrangente, baseada na compreensão de que a própria sociedade é objeto de segurança e deve fornecer salvaguardas e respostas adequadas. As conceituações estonianas de cibersegurança nacional, defesa psicológica cibernética e comunicações estratégicas são elaboradas à luz de situações reais de ameaças seminais. A análise da evolução dos documentos estratégicos orienta as recomendações para uma mistura ainda mais profunda da cultura técnica de segurança cibernética com a defesa psicológica centrada em valores e a internacionalização da consciência situacional e do planejamento da segurança da informação.

Palavras chave: *Estônia; Rússia; Ameaças híbridas; Cyber; Defesa psicológica; Comunicações estratégicas (stratcom); Warfar de informação;, Ambiente de informação; Ciberespaço; Arma de informação; Arma cibernética; Cíber segurança*

1. Introduction

The current case study elaborates Estonian comprehensive approach to national security. Specifically, the informational instrument of power in international relations and measures to secure domestic information environment are scrutinized.

A suitable theoretical framework for analysis emerges from the Copenhagen school widened approach to security and societal security concept (Chifu, *n.d.*). The notion of having society as the object of security echoes loudly in analysed national security documents and in practical application of strategy in the fields of cybersecurity, psychological defence and building resilience against hybrid threats.

The authors have knowingly omitted force comparisons of realist schools' hard security approach. Threats emanating via information environment deserve attention in this scope as far as they can be considered political threats in the Buzanian terms (Buzan, 1991: 118-123). On several occasions technically similar

situations that cybersecurity and psychological defence are set to build resilience against, can occur as consequences of natural emergencies, a sophisticated crime or a manifestation of some ill-advised comments in the public information sphere. In that sense, the distinction between generic malware and cyber weapons from consequential, political and legal perspectives as described by Thomas Rid (2013: 46-47) define if something deserves a national security label.

The *raison d'être* of the Republic of Estonia is declared in the preamble of the Estonian constitution, 'which must guarantee the preservation of the Estonian people, the Estonian language and the Estonian culture through the ages' (1992). Barry Buzan highlights social vulnerabilities and threats that as 'matters of language, religion and local cultural tradition all play their part in the idea of the state', hence deserve protection from state against hostile impacts to societal security (1991: 123, 19). This kind of securitization is not absolute and normally is not governing gradual linguistic development by loans, evolutionary development of peaceful subcultures, changes of individual religious beliefs among population or vivid cultural life far beyond traditional folk music and dances.

In recent years, there have occurred a heated public and academic discussion of "hybrid warfare" or "hybrid threats"— and on a number of closely related concepts, some with precise definitions and some rather vague (e.g. election meddling, fake news, subversive leverage, information disorder, asymmetric war(fare), fourth-generation warfare, non-linear war(fare), non-traditional warfare, the 'Gerasimov doctrine', gray zone activities). This article does not seek to give any new definitions for the phenomenon itself, as authors agree with the European Commission, which has stated:

> While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity

to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats (European Commission, 2016).

As seen here, the concept involves both technological (including cyber) and psychological vulnerabilities of a possible target country, therefore, the defence should also contain both these domains.

The most probable adversary using hybrid set of leverage means in the case of Estonia would be Russia. The Russian point of view was essentially defined in a speech and in an article by the head of General Staff Valery Gerasimov in 2013. It is worth noting that already then conflicts were considered to be a permanently ongoing process and not a theoretical occurrence of the future (Gerasimov, 2013). Both points have become more concise in latest iteration of official Russian military doctrine (Kremlin, 2014).

For the sake of clarity academic, working definitions of relevant concepts used in current article are provided as follows.

Information environment – IE is comprised of the information itself, the individuals, organisations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs (MC 0422/6, 2018: B-1). Dynamic physical and/or virtual settings interpreted by the mind (StratCom COE, 2019: 30).

Cyberspace - time-dependent set of interconnected information systems and the human users that interact with these systems (Ottis & Lorents, 2010).

Information weapon – selected or created targeted information, propagated logical framework or a viral text intended to influence perception, judgements or behaviour of a target in the context of information conflict.

Cyber weapon – programs, equipment, tactics, techniques, and procedures used for offensive cyber operations (Growther, 2017); computer code that is used, or

designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems, or living beings (Rid, 2013: 37).

Strategic communications (*stratcom*) - A holistic approach to communication based on values and interests that encompasses everything an actor does to achieve objectives in a contested environment (StratCom COE, 2019: 31).

Psychological defence – development, preservation, and protection of common values associated with social cohesion and the sense of security (Estonian Parliament: 2010).

National Cybersecurity – state of having national security safeguarded from threats emanating from network and information systems. (Estonian Ministry of Economic Affairs and Communications, 2019: 40).

Information War(fare) would not be hereby defined as the concept has developed into too variative discourses from overenthusiastic proponents on reform in military affairs similar to advocates of air power in 1920s, from battlefield technicalities to geostrategic conceptualisations or to dystopias on fundamental alteration of human societies (Szafransky, 1995; Arquilla, 2007, p. 7-8; Potšeptsov, 2009). Although in public debates on societal security 'information war' is often mentioned, the concept has defuncted among Western doctrine development and academic research circles.

2. Method

The narrative case study method is applied to study the intertwined wend of two conceptual security disciplines in Estonia. The case study approach has a relatively long history in humanities and social sciences.

For modern qualitative analysis one of the founding fathers of respective contemporary research methodology Robert K Yin (2013) describes the essence of case study as 'an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and con-

text are not clearly evident, and in which multiple sources of evidence are used' (p. 23). Bogden and Bilken (2003) define case study as "a detailed examination of one setting, or a single subject, a single depository of documents, or one particular event" (p. 54).

Narrative research originated from literature, history, anthropology, sociology, linguistics. Since the late 1980s and 1990s, research in the social sciences has taken "a sharp turn to narrative" (Clandinin, 2013, p. 10). Narrative approach is utilized here to provide a dynamic perspective of inferentiality in the chronological order of the key events throughout the timeline of concepts.

In our overview, there are two cases provided: (1) the cyber case – from prime school educational digitalization of 'the Tiger Leap' to world forerunner of cyber security; (2) the psychological defence case – from accommodation of constant attacks against ontological security of the state to recognized comprehensive psychological defence model securing national identity and building societal resilience. As the progress of the same protagonist (and in current case, the same antagonist) in the narrative evolves in the same timeframe, it would be useful to study the cases together.

3. Development

3.1. Cases of realisation of information-related hybrid threats in Estonia

Hostile influence activities against Estonian nation's popular aspiration for regaining independence from the East did not cease with the collapse of the Soviet Union. Nonetheless, dealing with active measures[1] of the Russian Federation were rather considered as matter of close professional counterintelligence circles not a central tenet of national security until 2017.

The crisis in Estonia in the spring of 2007 that escalated around the World War II memorial known as the Bronze Soldier statue is remembered in Estonia mostly due to two nights of rioting in the capital. Abroad the main emphasis has been on the first

ever cyber-attacks conducted by one country against another (Singer & Friedman, 2014). The first signs of coordinated Russian action could be noticed in January 2007, when diplomatic pressure and high levels of media coverage began and, probably, the secret services received their marching orders. In March and April, semi-clandestine meetings were detected between one of the leading figures of the soon-to-be rioters and Russian diplomats. By April tensions were high and on 26 April these escalated to rioting of a mainly Russian-speaking crowd. The following days witnessed economic and diplomatic pressure from Russia (even a demand for the Estonian government to resign), a blockade and attacks on the Estonian Embassy and on the Ambassador in Moscow by members of a pro-Kremlin youth organisation, and aggressive media coverage. Activity in social media—then still in its infancy, consisting of forums and below-the-line commentaries on the websites of media outlets—was extensive and included the use of a doctored image showing the iconic statue of the Bronze Soldier being cut up. Cyber-attacks on Estonian state institutions and businesses (notably the media and the banks) began sporadically on 27 April and were followed by four massive waves on 4 May, 8–10 May, 15 May and 18 May. (Juurvee & Mattiisen, 2020).

Such mixture of leverages – what now is called 'hybrid' – was new at the time. The nature of cyber-attacks was changing and their intensity grew from relatively simple means, even earning the label "cyber riots", to more dangerous DoS (denial of service) attacks and finally well-coordinated DDoS (distributed denial of service) attacks. (Tikk, Kaska & Vihul, 2010).

Next time the politically motivated cyber-attacks were noticed in Estonia was during the NATO military exercise *Steadfast Jazz 2013* that followed Russian exercise in Western Military District *Zapad-13*. On 7 November 2013 a defacing attack against the Estonian railway company Elron – the sole company providing local passenger train connections in the country¬– occurred. It stated everybody visiting the website in clumsy and erroneous Estonian: "*Train traffic in Estonia has been cancelled: Due to ongoing NATO exercises Steadfast Jazz 2013 the railway traffic and passenger services are temporarily cancelled*" (Kaukvere, 2013). On the next day a number of organizations received a fake email on behalf of the head of NATO Cooperative Cyber Defence Centre of Excellence situated in Estonian capital Tallinn, with strange content, claiming that Centre is carrying out information se-

curity audit of their organization as a part of the exercise Steadfast Jazz (Kovacs, 2019). At the same time DDoS attacks went off against targets in Estonia, Latvia, and Ukraine. Russian media misleadingly attributed the attacks to CCDCOE as a part of a NATO exercise gone wrong (ICDS, 2013).

Although Estonia has later faced some potentially serious cyber-attacks – most notably against VKG chemical products concern possibly originating from APT28 aka Russian military intelligence (Estonian Information System Authority, 2016, 23; FireEye, 2014) – these have not been used in coordination with other components of hybrid leverage. The advanced use of cyber means for influence activities has been confronted continually. One example is from January 2019, when Facebook removed 364 "pages and accounts for engaging in coordinated inauthentic behaviour as part of a network that originated in Russia", some of them where operating against target audiences in Estonia. Facebook Head of Cybersecurity Policy noticed that "despite their misrepresentations of their identities, we found that these Pages and accounts were linked to employees of Sputnik, a news agency based in Moscow, and that some of the Pages frequently posted about topics like anti-NATO sentiment, protest movements, and anti-corruption" (Gleicher, 2019).

Influence operations and cyber-attacks have held protuberant place in public threat perception within the dozen years following the 2007 Bronze Soldier crisis as national security polls reflect (Estonian Ministry of Defence, 2020).

During the first wave of COVID-19 pandemic Estonians considered information-related threats among the most pressing to Estonia. From the respondents to a national security poll 87% considered cyber-attacks being a threat of major or some extent to peace and security of Estonia. Proliferation of disinformation and fake news earned same rating. Spread of epidemics and global economic crisis were referred just 4-5% more (Turu-Uuringute, 2020: 16).

3.2. Strategy documents: cyber security, psychological defence, strategic communications

The National Security Concept (NSC) 2010, adopted by the Parliament in May 2010, introduced a change in security thinking although the roots can be traced

back to earlier documents. It stated that "Estonia's security policy is based on a broad concept of security, entailing all trends affecting security and essential areas required for ensuring security." The analysis of security environment had changed substantially since adoption of previous NSC and becoming a NATO member in 2004. According to NSC 2010, Estonia as a democratic, open society could be affected by the spread of extremist, hostile or hate-based ideologies. Such tendencies might weaken social cohesion, reduce tolerance and cause social tension. According to document in the environmental context of open and free media the "attacks against cohesion of Estonian society necessitate greater attention to the sense of cohesion and psychological defence." Uneven regional development and poorly adapting social groups could affect internal stability. The strengthening of civil society and the continuity in integration process were seen as reinforcing factors of Estonia's security. The answer to such vulnerabilities had to be broad. The document defined six pillars of the national defence that would be implemented comprehensively and were more-or-less the same as are in force now: military defence, civil contribution to military defence, international activity, ensuring of internal security, securing the resilience of critical services, and psychological defence (Estonian Parliament, 2010). From the point of view of this research paper psychological defence is hereby the most important since it is dealing directly with society's resilience or "*kerksus*" in Estonian, as it is known now (Juurvee, 2018).

The document stated that psychological defence is emanating from constitutional values and serves to enforce Estonia's security thus defining the foundations and general aim. NSC 2010 also gave a more precise definition: "Psychological defence is the development, preservation and protection of common values associated with social cohesion and the sense of security." The aim of psychological defence was foreseen as safeguarding the security of the state and the society, enhancing the sense of security, averting crisis and increasing trust amongst society and towards the actions taken by the state. Psychological defence had to facilitate the strengthening of "nation's self-confidence and the will to defend Estonia." Psychological defence and the recognition of constitutional values were to strengthen the resilience to avert anti-Estonian subversive activity. Additionally the document foresaw the development of psychological defence in co-operation with "all members of civil society." NSC 2010 named harmonized regional devel-

opment and integration also as fields of internal security (Estonian Parliament, 2010).

Although adopted on the highest possible level – the Parliament – NSC 2010 still did not provide the public service and society in general precise instructions for building up the psychological defence. Such guidelines were provided by the Government of the Republic in a document adopted at the last day of the very same year: the National Defence Strategy (NDS), valid since 1 January 2011. NDS foresaw three main lines of action for psychological defence:

a. Identifying hostile influences and protecting against them;
b. Rising the endurance of public broadcasting services relevant networks are attacked;
c. Enhancing the public will to engage in defence and the popularisation of security-related thinking (Estonian Government, 2010).

NDS 2011 also pointed out aspects of psychological defence that should be taken into account when developing the following fields:

a. Notifying the population of the risks and developing its knowledge and skills for crisis situation;
b. Solving emergency situations and informing the population in such situations;
c. Improving Estonia's international image.

The document also set responsibilities and stakeholders for planning of the filed. The Government Office became the coordinator and contributors were the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Culture, the Ministry of Education and Research, the Ministry of the Interior, the Rescue Board, the Defence Forces and national security institutions (Estonian Government, 2010). While such list in general makes sense, oddly enough the Ministry of Social Affairs was not included.

The activities envisioned in the documents did stay on paper only. Although the information in public domain is limited there are some public references of developments in public reports. In the following years the possible threats were analysed and requirement raising from the analysis were integrated into political and operational planning, manuals, training system and exercises. Psychological defence was developed in international cooperation and involving the domestic public, organizing different conferences and workshops to meet that end (Estonian Ministry of Foreign Affairs, 2013, 2). Members of civil society, academics, journalists and public servants discussed the topic in the newly formed format of Psyhological Defence Courses (Arold, 2014).

The public discussion about psychological defence started already in March 2011 as a reaction to the article "People and nations have a right for informational self-determination" by the member of the Estonian Academy of Sciences and the Minister of Defence Jaak Aaviksoo (Aaviksoo, 2011). Following debate in press was rather heated and although it soon lost its momentum, its implications cannot considered to be over, yet. Academic study of the discussion was conducted several years later in 2015 using in-depth interviews with public servants, journalists and opinion-leaders, some of whom had been actively expressing their opinions on the press. It concluded that in general there was an agreement that the concept of psychological defence is needed and its main idea is to protect the mentality and values of Estonias' society against hostile information-based (influence) operations. Respondents found that coherent actions should be carried out by security and communication professionals and these should reinforce community's value system. On the other hand, the abstraction of psychological defence was not understood unambiguously by Estonian security policymakers (Narits, 2015).

Next phase of active public discussion on the societal resilience in Estonia followed the Russian military action in Ukraine in 2014. Although some new terms like *hybrid warfare* appeared in discourse, it did not provide securitization of new fields that would concern this research paper. Rather the arguments pointed out in 2007-2010 were repeated and dealt in more concise form. While dealing with the topic in 2014 the adviser of the Government Office pointed out, that for public servants psychological defence means awareness of current informational threats

while writing planning documents, comprehensiveness of exercises and public engagements, and keeping in mind the preamble of the Constitution. He also underlined the contribution of each citizen, because everybody could be exposed to direct or indirect hostile influences that should be recognized in order to avoid becoming an *useful idiot*[2] spreading panic or disinformation (Arold, 2014).

European refugee crisis starting in 2015 influenced public discourse in Estonia and contributed to securitization of manifestations of intolerance (Raag & Günter, 2016). Such debates found their way to doctrinal documents with speed that was unseen previously. New version of the NSC adopted in 2017 does not change the essence of the previous NSC 2010. The comprehensive approach to security remains central in NSC 2017. However, it successfully describes the main current challenges for societal security. Uneven regional development, social inequality, poverty, poorly adapted segments of society or manifestations of intolerance were seen as factor that could affect the stability of the state. The polarisation of society due to adversarial opinions and understandings were pointed out as situation that increases uncertainty and decreases society's resilience. The document has a special chapter (3.8) dedicated to resilience and cohesion of society which provides narrower focus for psychological defence and introduces a new term - strategic communication (Estonian Parliament, 2010).

Estonia considers itself as a digitally advanced country. According to World Bank estimations Estonia is among one of the handful countries becoming *truly digital society*. (Ross, 2016, pp. 5, 248; World Bank, 2016, pp. 17,54). According to the National Cyber Security Index, Estonia is ranked No. 3 in among 160 states. Voluntary societal engagement in crisis preparedness on the field of cyber security deserves furthermost distinction (NCSI, 2020). Cyber enthusiasm has not always been thoroughly accompanied with realisation of risks accompanied with digitalization of governmental and commercial services.

The cyber defence, although mentioned in the National Security Concept, used to be more widely covered in different documents. Again, the main motivator behind these documents were the cyber-attacks in spring 2007 – until then the documents dealing with development of information infrastructure did not go further than just mention-

ing the importance of security. The major step forward was the Cyber Defence Strategy 2008-2013. The document contains a wish-list for future developments and defines the aim of cyber security as "decreasing vulnerability of cyber domain of the state as whole" (Estonian Government, 2008). The next iteration of the document foresaw the objective for next four years as "increase[ing] cyber security capabilities and people's awareness of cyber threats to ensure continued confidence in cyberspace" thus binding the psychological defence and cyber defence together (Estonian Ministry Economic Affairs and Communications, 2013). In the third iteration of the document, in force during writing of this article, the desired state of affairs by 2022 was defined followingly: "Estonia is a sustainable digital society with strong technological resilience and crisis preparedness" (Estonian Ministry Economic Affairs and Communications, 2017).

Current Estonian national security concept is rather descriptive in its language. Therefore, it is possible to identify highlighted components and vivid priorities of information-related security disciplines from the time of approval, but not definitions. Strategic communications and psychological defence are described as complemented disciplines dealing with the societal fabric and communicative realm. Strategic communication (stratcom) provides generic communicative prism to all words and deeds of the executive branch of state power. Effectiveness of stratcom is built upon societally negotiated formulation of democratic values for the sake of national cohesion. Notion on stratcom as a dialogue platform with society considers domestic population as its stakeholder as well as its target audience.

The core of psychological defence is defined around protection of constitutional values that implicitly are non-negotiable. The set of measures described in the concept do not limit psychological defence with communicative means only, as it includes prevention and neutralisation of publicly insinuated armed insurgencies with domestic or imported origin. This is to be done together with civic society stakeholders. However, if possible, threats are preferably mitigated just by exposing them by public education. (Estonian Parliament, 2017).

The official document does not contain any schematic. In academic literature this is still available. Most often described scheme of psychological defence is depicted on Figure 1 (Rebane, 2009; Jantunen, 2015: 316; Arold: 2020).

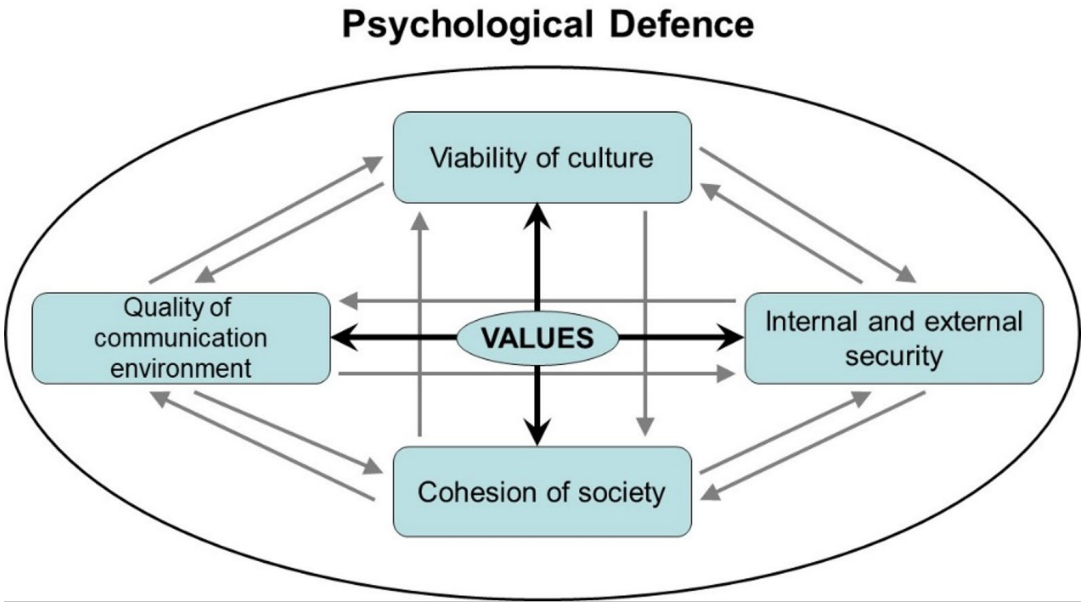

Figure 1: *Estonian psychological defence model.*

In the model constitutional values have the central stage. Wide acceptance of constitutional values enables other societal security components relevant to psychological defence. All other components are vulnerable from weakening of other components. In this paradigm role of cybersecurity is reflected as systematic technical enabler for quality of communication environment. Strategic communication capability has its play in formation of internationally intertwined security setup (by consolidating instruments of power for communication effects).

Functions of strategic communication and cybersecurity in the context of constitutional values does not provide the full picture, yet. In the quality of communication environment self-regulatory mechanisms play the pivotal role. Editorial independence and professionalism of private and public media are quintessential. There is no law on journalism in Estonia. However, self-regulatory traditions covering public and competing private media houses are strong.

For the sake of cybersecurity minimizing number of vulnerable computer users is propagated under cyber hygiene label from the very beginning, and not only in coding classes for 7-year-olds (Olson, 2012). In a wider context, importance of information hygiene (media literacy + cyber hygiene) is instructed. It is advised not to be 'contaminated' with fake news and become an involuntary disseminator (an 'useful idiot') of viral texts/memes or computer viruses. (Kahar, 2008; Rebane 2019: 165-173, Vaarik: 2014: 260, 268-275, Arold, 2015).

Viability of culture (preservance of national identity) is the unavoidable prerequisite for any strategic communication plans and psychological defence measures as the constitution and national security concept prescribe. However, modern founding fathers could not have foreseen that being a digitally highly capable nation forerunning international cybersecurity agenda might attain such a prominent role as a national identity marker. Importantly, this has been the consequence of consensual narrative framing of cyber-attacks of 2017 (Clarke & Knake, 2010: 11-17,20; Rebane, 2020; Alenius, 2013).

Cohesion of society describes not just ends of the strategy. It involves enhancement of number of societal human links (both technologically moderated and analogous) in order to advance societal integration and to strengthen endurance of the society as a system.

3.3. Institutional evolution of dealing with cyber threats

Although Estonia had paid much attention on ICT developments already in 1990ies, the security issues were addressed through the prism of data protection (Siil, 2001). Even after the major reorganization started in 2003 that ended with creation of new official body the Estonian Informatics Development Centre, only one of its core functions was "organization of activities connected to data protection in the state information systems" (Estonian Minister of Economy and Communications, 2005). Break-through on institutional sense was establishing Estonian Computer Emergency Response Team (CERT-EE) at the beginning of 2006 – it was done well prior to the 2007 cyber-attacks, not vice versa. As the Permanent Undersecretary of the Estonian Ministry of Defence has recalled, the intelligence services had predicted

a cyber-attack taking into account the high reliance of Estonia on e-services, however, these were not forecasted for late April, but rather for March 2007 when the first internet voting on parliamentary elections took place in Estonia. The solution from Estonian Government was cooperation between different state and private entities, especially banking sector (Mansfield-Devine, 2012).

In the military domain cyber defence evolved on different pace. In late 2003 Admiral Edmund P. Giambastiani, head for the Allied Command Transformation visited Estonian Commander of Defence General Johhannes Kert. At the time NATO was initiating establishment of network of Centres of Excellence (CoEs) and Admiral mentioned that Estonia, known for its IT know-how should show some initiative in the field of cyber defence. General Kert was eager to seize the chance. In the following year the idea was refined and lobbying done both in- and outside Estonia. The building for the soon-to-be NATO CoE was finished already in 2006 (Kaljula & Suurkask, 2019). At the same year the concept of Cooperative Cyber Defence CoE proposed by Estonia in 2004 after joining NATO, was approved by Supreme Allied Commander Transformation. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was officially established in Tallinn on 14 May 2008. The North-Atlantic Council gave full accreditation and status International Military Organizaton to the Centre in October the same year (NATO CCD COE, 2020).

As shown above, the 2007 cyber-attacks did not initiate the foundation of CERT-EE and NATO CCD COE, oddly enough the decisions had been made well prior to these attacks. However, they certainly gave some boost to the topic of cyber defence both domestically and internationally. While the earlier cyber-attacks targeting private business were frequently kept quiet about by the victims, this time the communication was much different – the incidence were widely talked about and such decision was made on the level of President, Prime Minister and Minister of Foreign Affairs. As former head of CERT-EE Hillar Aarelaid has pointed out, "Without the events of 2007 we would not have been able to connect Estonia with the topic of cyber defence" (Lõugas, 2017). Therefore, through orchestrated approach to communication fencing off the cyber-attacks became an important tool of communication itself.

Later years have provided only one major structural chance with reorganizing Estonian Informatics Development Centre into Information System Authority (although different names in English, they seem rather similar in Estonian and even share the same abbreviation – RIA – that may cause some confusion) in 2011. Compared to earlier, the importance of *security* among the functions of RIA had considerably raised. In 2011 CERT-EE was listed on the seventh place among the ten functional departments of the Information System Authority (Estonian Minister of Economy and Communications, 2011). Continuation of such trend is clearly visible in the next iterations of the Authority's statute, by 2020 it takes the first place among the 12 functional departments listed in statute (Estonian Minister of Economy and Communications, 2020).

4. Conclusions

Estonian approach to the cerebral aspects of information security looks vital in its comprehensiveness. However, official conceptualisation fails to explain the rationale of building psychological defence and executing strategic communication in parallel veins. Both functions are essentially planned and co-ordinated by the same office and seek similar ends. Distinction of ways and means between the disciplines looks artificial. Strategic Communication principles could be practically extended to non-securitized areas of policy planning. Psychological defence as an essentially security function has deeper roots in the legislative history, but is built on a more contested ground as a more innovative and precedential notion compared to other states' security setup. It would be advisable to use term 'strategic communications' for governmental communication practices that contribute to informing policy decisions, while reserving psychological defence as a sole notion for securitized communicative decisions and capability development.

The national security concept frames cybersecurity, psychological defence and strategic communication through same lanes as a matter of resilience – preparation, endurance and ability to revitalize in case of attacks. However, development of cyber security according to national security strategy is rather technical and does not account notions of cultural impacts. Psychological defence as a societal security concept is not precise enough to inform message and platform related issues in the digital realm.

Informatization of contemporary societies prescribe closer integration of the functions. It is understandable, that cyber as a conflict domain could not become an independent key pillar of national defence (otherwise Estonia should consider comprehensive naval, airspace and ground securities according to the same logic). As the definitions of information environment and cyberspace, information weapon and cyber weapon, strategic communications / psychological defence and national cybersecurity hint, *cyber* is generally a subset of *information* and the challenges of information warfare should be met with joint information security. In this context system-centric cyber-defence and value-centric psychological defence complement each other.

There is already a 3rd iteration of cyber security strategy in force in Estonia. The authors were not able to identify continual doctrinal process for psychological defence. Cyber security strategy considers national cybersecurity in a globalized world, deals with Estonian positions regarding jurisdiction and legal norming of malicious cyber activities. In essence, context of cybersecurity is the world.

Psychological defence in 2010 national defence strategy does have a say about the playground being borderless media space where threats emerge and effects are gained. The latest national security concept permits psychological defence means to be international, whereas strategic communication is limited to own society during state of normality. The objective information environment remains the same for technical and cultural influences. Therefore, considering not only possible threats, but capability building and operations in international arena would make sense.

Estonian case study on securitization of communication and means of communication provides insight on reasons why system-centric and value-centric policies have developed in different veins.

The uncontested need for cybersecurity in a digitally dependent society has resulted fast-track conceptual developments pioneering even on global scale.

Obviously, value-centric psychological defence needs more time to mature in the societal establishment and would probably remain slightly controversial forever, at least in the eyes of conspirologists, agents of influence and *useful idiots*.

References

Aaviksoo, J. (2011) *Inimestel ja rahvastel on informatsioonilise enesemääramise õigus* [People and nations have a right for informational sovereignty] https://www.diplomaatia.ee/artikkel/infokonfliktid-ja-enesekaitse/

Alenius, K. (2013). Victory in Exceptional War: The Esonian Main Narrative of the Cyber Attacks in 2007. In:Rantapelkonen, J., Salminen, M. (2013). The Fog of Cyber Defence. Helsinki: National Defence University. pp. 85-94.

Arold, U. (2014) *Eesti psühholoogilise kaitse kasvamislugu* [The evolution of Estonian psychological defence] https://www.postimees.ee/2931583/eesti-psuhholoogilise-kaitse-kasvamislugu

Arold, U. (2020). Estonian Psychological Defence against Russian Influence Activities. In: Lochard, I.V. (Ed.). "Information-Related Hybrid Threats." *NATO Science for Peace and Security Series E and Societal Dynamics*. IOS Press: Amsterdam, 2020 (forthcoming).

Arold, U. (2015), 'Infosõja mõistatus' [Mystery of information war], Kaja, Kommunikatsiooni ja suhtekorralduse ajakiri, vol. 18, pp. 9–14.

Arquilla, J., (2007). Information Strategy and Warfare. A guide to theory and practice. New York and London : Routledge.

Bogdan, R. C., & Biklen, S. K. (2003). Qualitative research for education: An introduction to theories and methods (4th ed.). New York, NY: Pearson Education Group.

Cambridge Dictionary. (2020). https://dictionary.cambridge.org/dictionary/english/useful-idiot

Chifu, I. (n.d.) *Societal security. An agenda for the Eastern Europe*. Center for Conflict Prevention and Early Warning. [Online] [Cited: 23.10.2018] http://www.cpc-ew.ro/pdfs/societal_security.pdf

Clandinin, D. J. (2013). Engaging in narrative inquiry. Walnut Creek, CA: Left Coast Press.

Clarke, R. A.& Knake, R.K. (2010). Cyber War. The Next Threat to National Security and What To Do About It. New York: HarperCollins Publishers.

Estonian Government (2008) *Küberjulgeoleku strateegia 2008–2013* [Cyber Defence Strategy 2008-2013] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

Estonian Government (2010) *Riigikaitse strateegia* [Natioanl Defence Strategy] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/riigikaitse_strateegia.pdf

Estonian Information System Authority (2016) *Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte* [Annual Report of Information System Authority's Cyber Security Service of 2016] https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-kuberturbe-aastaraport-2016.pdf

Estonian Minister of Economy and Communications (2005). *Riigi Infosüsteemide Arenduskeskuse põhimäärus* [Statute of Estonian Informatics Development Centre], https://www.riigiteataja.ee/akt/830212

Estonian Minister of Economy and Communications (2011). *Riigi Infosüsteemi Ameti põhimäärus* [Statute of Estonian Information System Authority], https://www.riigiteataja.ee/akt/128042011001

Estonian Minister of Economy and Communications (2020). *Riigi Infosüsteemi Ameti põhimäärus* [Statute of Estonian Information System Authority], https://www.riigiteataja.ee/akt/125032020010

Estonian Ministry Economic Affairs and Communications (2013) *Küberjulgeoleku strateegia 2014–2017* [Cyber Defence Strategy 2014-2017] https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

Estonian Ministry Economic Affairs and Communications (2019) *Küberturvalisuse strateegia 2019–2022* [Cyber Defence Strategy 2014-2017] https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

Estonian Ministry of Defence. (2020) *Avalik arvamus ja riigikaitse*. [Public opinion and national defence] https://www.kaitseministeerium.ee//et/eesmargid-tegevused/avalik-arvamus-riigikaitsest

Estonian Ministry of Foreign Affairs (2013) *Ülevaade Eesti julgeolekupoliitika aluste (2010) elluviimisest* [Overview of implementation of National Defence Concept 2010] https://vm.ee/sites/default/files/content-editors/JPA_2010_elluviimisest.pdf

Estonian Parliament (2010) *Eesti julgeolekupoliitika alused* [Estonian National Security Concept] https://www.riigiteataja.ee/aktilisa/0000/1331/4462/13316508.pdf

Estonian Parliament (2017) *Eesti julgeolekupoliitika alused* [Estonian National Security Concept] https://riigikantselei.ee/sites/default/files/content-editors/Failid/national_security_concept_2017.pdf

European Commission (2016) *Joint Framework on countering hybrid threats: a European Union response* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

FireEye (2014) APT28: A Window Into Russia's Cyber Espionage Operations? https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Gerasimov, V. (2013) Ценность науки в предвидении [The value of science in foresight] https://vpk-news.ru/articles/14632

Gleicher, N (2019) *Removing Coordinated Inauthentic Behavior* from Russia, https://about.fb.com/news/2019/01/removing-cib-from-russia/

Growther, G.A., (2017). Cyber weapon. [book ed.] Springer, P.J., 2017. Encyclopedia of Cyber Warfare. Santa Barbara, CA, Denver, CO : ABC-CLIO.

ICDS (2013) *The DDoS and Defacement Attacks of "Anonymous Ukraine" and "CCD COE": interactions between "patriotic" hackers, media and political leadership in cyberspace*, November 12, 2013, https://icds.ee/en/the-ddos-and-defacement-attacks-of-anonymous-ukraine-and-ccd-coe-interactions-between-patriotic-hackers-media-and-political-leadership-in-cyberspace/

Jantunen, S. (2015). Infosota. "Iskut kohdistuvat kansalaisten tajuntaan." [Information war. "The attack on the people's consciousness"] Helsinki : Kustannusosakehtiö Otava.

Juurvee, I. (2018) Estonia's approach to Societal Security. [eds.] Aaltola, Mika, Kuznetsov, Boris, Sprūds, Andris, Vizgunova, Elizabete. *Societal Security in the Baltic Sea Region. Expertise mapping and raising policy relevance*. Riga : Latvian Institute of International Affairs, 2018. pp. 100-117.

Juurvee, I. & Mattiisen, M. (2020) The Bronze Soldier Crisis of 2007: Revisiting an early case of hybrid Conflict, ICDS Report, https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf

Kahar, A. (2008). *Ärgem olgem "kasulikud idioodid"*. [Let's not be 'useful idiots']. Eesti Päevaleht. https://epl.delfi.ee/arvamus/andres-kahar-argem-olgem-kasulikud-idioodid?id=51141127

Kaljula, R. & Suurkask, H. (2019). Sidepataljoni 100 aastat: Traadita telegraafist küberväejuhatuse loomiseni, 2. osa. [100 Years of Communication Battalion: From Wireless Telegraphy to the Establishment of Cyber Command. Part 2]. Tallinn: Küberväejuhatuse staabi- ja sidepatajon.

Kaukvere, T. (2013) *Häkkerid teatasid rongiliikluse peatumisest* [Hackers report train traffic halted], *Postimees*, 7 November, https://tarbija24.postimees.ee/2588982/hakkerid-teatasid-rongiliikluse-peatumisest

Kovacs, E. (2013) *Mysterious NATO Cooperative Cyber Defence Centre of Excellence Spam Spotted: Conrad Longmore of Dyanmoo's Blog has analyzed the emails, Softpedia News*, 5 November, https://news.softpedia.com/news/Mysterious-NATO-Cooperative-Cyber-Defence-Centre-of-Excellence-Spam-Spotted-397213.shtml

Kremlin (2014) Президент утвердил новую редакцию Военной доктрины [The president approved new version of Military Doctrine]. Kremlin.ru. 26 December, http://kremlin.ru/events/president/news/47334

Lõugas, H. (2017) *Pronksiöö10: küberrünnakute müstifitseerimine oli teadlik käik* [Bronze Night 10: Mystification of Cyber Attacks Was a Deliberate Move]. Digigeenius, https://digi.geenius.ee/rubriik/uudis/pronksioo10-kuberrunnakute-mustifitseerimine-oli-teadlik-kaik/

Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. Network Security, July 2012, 12-20.

MC 0422/6 (2018) NATO Military Policy for information operations, https://shape.nato.int/resources/3/images/2018/upcoming%20events/MC%20Draft_Info%20Ops.pdf

Mitrokhin, V. (2002) KGB Lexicon: The Soviet Intelligence Officer's Handbook. London : Franck Cass.

Narits, T. (2015) P*sühholoogiline kaitse eesti julgeolekupoliitika kujundajate käsitluses. Magistritöö*. [Understanding of Psychological Defence by Security Policymakers. MA Thesis] Tallinn : Sisekaitseakadeemia https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/20/2015_Narits%20.pdf?sequence=1&isAllowed=y

NATO CCD COE (2020). *History*. NATO CCD COE official website, https://ccdcoe.org/about-us/

NCSI. (2020) National Cyber Security Index: Estonia. https://ncsi.ega.ee/country/ee/

Olson, P. (2012) Why Estonia Has Started Teaching Its First-Graders To Code. Forbes. 06.09.2012.

Ottis, R; Lorents, P. (2010). Cyberspace: Definition and Implications. *Proceedings of the 5th International Conference on Information Warfare and Security: 5th International Conference on Information Warfare and Security, Dayton, Ohio, USA, 08-09.04.2010*. Ed. Dr Leigh Armistead. Reading, UK: Academic Conferences Limited, 267–270. https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf

Potšeptsov, G., (2009). Strateegiline sõda. [Strategic war] Tallinn : Infotrükk.

Raag, I. & Günter, A. (2016) *Eesti strateegilise kommunikatsiooni kilde 2015-2016* [Fragments of Estonian Strategic Communication] https://www.propastop.org/wp-content/uploads/2016/07/Eesti-strateegilise-kommunikatsiooni-kilde-2015-2016-1.-osa.pdf

Rebane, R. (2019). Hirmust eduni. Meediasuhtluse 8 reeglit. [From fear to success. 8 rules of media engagements]. Tallinn: Stratkom OÜ.

Rebane, R. (2020). Personal interview. Interviewed by Uku Arold 16.09.2020.

Rebane, R. (2009). *Kultuur kui viimane kaitseliin* [Culture as the last line of defence], Eesti Päevaleht. Riigi Kaitse, 23.12.2009.

Rid, T., 2013. Cyber War Will Not Take Place. London : Hurst & Company.

Ross, A. (2016) The Industries of the Future. New York – London – Toronto -Sidney : Simon & Schuster.

Szafranski, R., 1995. A Theory of Information Warfare. *Airpower Journal*, Spring 1995.

Siil, I. (2001). *The Estonian Informatics Centre – Five Years of IT Development*. Baltic IT&T Review, 24, 11-14.

Singer, P.W., Friedman, A., 2014, Cybersecurity and cyberwar. What everyone needs to know. New York: Oxford University Press, Amazon Kindle Book, loc. 2267-2368.

StratCom COE. (2019) Improving NATO Strategic Communications Terminology. Riga: NATO StratCom COE.

The Constitution of the Republic of Estonia. (1992). Passed on referendum 28.06.1992. https://www.riigiteataja.ee/en/eli/ee/530102013003/consolide/current

Tikk, E; Kaska, K & Vihul, L. (2010) International Cyber Incidents: legal Considerations. Tallinn: CCD COE.

Turu-Uuringute AS. (2020) Avalik arvamus riigikaitsest. Mai 2020. Aruanne Kaitseministeeriumile. [Public opinion on national defence. May 2020. Report to the Ministry of Defence]

Vaarik, D. (2014). Sõnumiseadja käsiraamat. [Handbook of a message manager]. Tallinn: Memokraat.

World Bank. (2016) Digital dividends. World development report. A World Bank Group Flagship Report. https://openknowledge.worldbank.org/bitstream/handle/10986/23347/9781464806711.pdf

Yin, R. K. (2013). Case study research: Design and methods. Thousand Oaks, CA: Sage.

Notes

[1] Active measures is a term from KGB vocabulary and was defined as "agent-operational measures aimed at exerting useful influence on aspects of the political life of a target country which are of interest, its foreign policy, the solution of international problems, misleading the adversary, undermining and weakening his positions, the disruption of his hostile plans, and the achievement of other aims." (Mitrokhin, 2002).

[2] Useful idiot – a person who is easy to persuade to do, say, or believe things that help a particular group or another person politically. (Cambridge Dictionary, 2020).