The Use of Cyber Activities as a Weapon: The Empirical Case of Ukraine

Christine Dugoin-Clement (Paris 1 Pantheon Sorbonne and

Centre de recherche écoles de Saint-Cyr Coëtquidan)

Abstract

Since the beginning of the war on its territory in 2014, Ukraine has experienced several waves of cyberattacks. Some have been conducted on the Internet, either through trolls and Twitter bots or via direct cyberattacks targeting critical systems. However, other techniques, such as "psyops" using cyber, have also been tested against Ukraine. In many documented instances, such operations have decreased trust in Ukrainian state institutions as well as public organizations and the military hierarchy. The present paper is based on field interviews in 2017 of military personnel and examines how, by means of cognitive dissonance methods, Internet-based attacks may be used to affect trained targets' behavior by increasing their level of uncertainty. Causing a decrease in specific targets' trust in their institutions or hierarchy enables their behavior to be changed.

The article addresses how these objectives are achieved. It also analyses the results of such attacks on a target—especially in terms of levels of trust—and how they deteriorate the target's cognition. Further, it examines how soldiers perceive being a target of Internet-based attacks using cognitive dissonance.

Introduction

Since the Maidan revolution in late 2013, Ukraine has faced war on its eastern territories in Donbass. This ongoing war is not only "kinetic" but has also included a large cyber warfare component. According to President Poroshenko, Ukraine faced 6,500 cyber-attacks on 36 Ukrainian targets between November and December 2017 alone. The attacks included classical intrusions on private and professional emails of persons of interest, as well as Distributed Denial of Service attacks (DDoS) of websites (including government). Larger-scale operations were also conducted, such as an attack on the electronic system used for the presidential election (May 2014) or power cuts affecting 225,000 people in 2015 and the Kiev blackout of December 2016.

Numerous operations targeting human psychology were conducted against Ukraine, notably on soldiers. Some of these operations used multifaceted tools to interfere with the robust cognition acquired by soldiers during training and to weaken trust in their hierarchy and government. The aim was to influence the subjects' behavior unbeknownst to them, a key issue this article will address.

In 2017, we conducted field interviews with active soldiers and veterans. The aim was to conduct a qualitative analysis in the light of cognitive dissonance theories (self-consistency and SSM model), a decision driven by the nature of the field and the specific profile of the subjects studied. Based on the 2017 interviews, we considered the question of whether Ukrainian soldiers' trust had been affected by cognitive dissonance deployed in Internet-based operations. In other words: had their perceptions changed and uncertainty increased enough due to Internet consumption to modify their behaviors? Another key question was to define whether they were aware of being potential targets or not.

Part I of the paper reviews the literature and defines some of the terminology, such as psyops, etc., and explains the theories used in the analysis, such as cognitive dissonance, and

trust in military affairs and in the Internet. Part II presents the Ukrainian case study, its methodology, the data collected, and our analysis.

Literature Review and Definition of Terms

Terms such as "cyber warfare" and "psyops" are often loosely defined due to their cross-disciplinary nature. As such, before presenting the theoretical framework we start the paper by defining relevant terms. This will help shed light on the data collected and analyzed, to be presented in Part II.

Clarifying the Terms

For Schaap, "cyber warfare" is "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and networks themselves, of another state" (Schaap 2009). Other definitions invoke "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke 2010). Still others divide cyber warfare into two types: strategic and operational. Strategic is explained as "a campaign of cyberattacks one entity carries out on another," while operational "involves the use of cyberattacks on the other side's military in the context of a physical war" (Libicki 2009). For the purpose of this paper, we use Schaap's definition of cyber warfare, as Libicki's refers to physical war by an identified adversary and as such is not applicable here.

In our case, although suspicions fall on Russia, final attribution of cyber operations is not absolutely defined. And while Clarke's definition involves a "nation-state," Ukraine faces both a separatist movement and cyberspace struggle against structures that are not all officially linked to a nation-state. Furthermore, the present paper addresses cyber operations having psychological effects on military staff rather than effects on computers or networks. Accordingly, we use the term "cyber operation" instead of "cyberwarfare." Moreover, our choice accords with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE).

This seems wise, given that the Ukraine conflict is linked to Russia's geopolitical strategy. The CCDCOE's definition (found in the Tallin Manual on the International Law Applicable to Cyber Warfare) denotes a broad approach and is defined as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace." Moreover, as the Tallinn manual is the result of a transnational study group, it makes sense to use its terminology.[1] Applied to the present subject, the CCDCOE's definition is large enough to embrace cyber psyops in a context of war, which matches our subject perfectly.

There is agreement among experts today that Ukraine was—and is—a test lab for cyber warfare operations and "psyops," or psychological operations (Greenberg 2017). When talking about psyops, we refer to operations aimed at influencing an enemy's state of mind through non-kinetic means. For this purpose, psyops can use chosen information or indicators to influence people's emotions, thoughts, and reactions. Targets will consequently change their minds and behaviors and, as fallout, the behavior of governments, organizations, or groups can also be changed. The word "psyops" first appeared in 1965 although the expression "Military Information Support Operations" (MISO) may also be used. On the Ukrainian information front, when addressing psyops, various channels were used to match the psychological profiles of targets, and the military was no exception. Concerning soldiers, stealth operations were conducted through the Internet, particularly social networks and chat forums. These operations targeted active fighters as well as veterans and used peer group trust to generate doubt and uncertainty toward the government and military hierarchy.

Existing Literature Review

[1] The Tallinn manual (*Tallinn Manual on the International Law Applicable to Cyber Warfare*, published in 2013 and followed by an updated version in 2017) was written on the invitation of the CCDCOE by a transnational group of IT experts and legal scholars. It deals with international law applications in cyber operations conducted by and directed against states, in cyber conflict and cyber warfare; as such, it had to define the terms covered by laws in this field.

By its very nature, the subject of the paper is at the crossroads of various theoretical frameworks. Due to their make-up, the operations studied require three different approaches. The methodology is based on cognitive dissonance and heuristic biases; the effects observed involved trust in military teams and military psychology; and the way messages are disseminated are essentially Internet-based, requiring channel-based trust.

Cognitive Dissonance and Decision Making

Although cyber operations use new technology, the methods of influence, such as persuasion or psychological destabilization, have been used before. Cyber tools, with their speed and opacity, are a way to designate a strategy, here based on cognitive dissonance. Developed in the 1950s by Léon Festinger, cognitive dissonance theory postulates that when two cognitions are opposed (said to be "irrelevant") in someone's mind, he or she will experience a "motivational psychological discomfort." The discomfort is "motivational" because in order to feel comfortable again, the subject will behave in such a way as to reinforce or weaken one of these cognitions. Aronson (1968, 1992) improved this theory by casting it in a more functional light. He developed the "self-consistency" variation, in which dissonance arises in people from contradictions between individual behavior/action and their perception of themselves. In this theory, the more people's perception of themselves is positive, or whose values are socially considered as positive, the more they will feel cognitive dissonance. And individuals whose lives are at risk are also more sensitive to cognitive dissonance (Jonas, Greenberg, & Frey 2003).

It seems clear that subjects such as soldiers match these prerequisites perfectly. Effectively, soldiers are associated with values perceived as highly positive, such as sacrifice for the greater good (related to heroic mythology), regularly putting their lives at risk, and facing extreme situations (that is, situations that are unpredictable, risky, and subject to rapid change). Further, empirical experience strengthens cognition. Since it helps soldiers stay

alive, training is validated by field experience and external operations (EOs). Training is therefore internalized, and soldiers follow it completely, consistent with Festinger (1956), for whom a cognition can be the result of past experience. In the case of soldiers, a cognition is initially learned during training, then later reinforced through validation by everyday life experience in extreme situations. According to theory, the more the cognition linked with their values is strengthened, the greater their reaction toward inappropriate behavior will be, functioning as an emotional reaction by-passing the thinking filter: more a reaction than a reflection.

Another relevant development of the theory is the Self Standard Model (SSM) of Stone and Cooper's integrative model (1999). In this version, the cognitive elements affected by dissonance may be personal standards (idiographic arousal) or normative standards (nomothetic arousal). In the case of soldiers, normative standards can turn into personal ones. On this basis, theoretically, they are highly sensitive to cognitive dissonance and thus to a potential cognitive attack. Indeed, cognitive dissonance incurred by psyops mobilizes soldiers' own standards to arouse dissonance—motivational discomfort—and make them change their behavior. These operations are highly effective when they decrease trust and certainty in soldiers' minds, thereby weakening the cornerstone of a properly functioning military, as we shall see in Part II.

With regards to the self-consistency model and Self Standard Model theory, the more a target is trained and conditioned, the more it can merge its professional values and self-perception, combining idiomatic and nomothetic standards. Consequently, training gives serious indicators on how soldiers think and react, thus helping in profiling. If the target is conditioned enough, we can postulate that this kind of profiling could be very effective and close to what a personal profile can be. Moreover, when reacting to a psyop built on cognitive dissonance, the target will not even be aware he had been influenced, as he changed

his behavior according to what he perceived as the very values and elements which are part of his personality, as highlighted by our interviewees' responses to their perception of being a target. Consequently, in professional settings, compromised personnel will not be easily detected because they are still loyal to the overall pattern of what must be defended and what is worth fighting for.

It seems clear that the risk component of a deterioration in trust is a change in behavior based on a change in decision-making. But making a realistic prediction of what the agent behavior could be in order to secure an organization strategy (i.e., being sure that orders are going to be executed without modification) implies the supposition that decision-making is based on rationality. The "rational choice model" refers to theories of action in this area of research. Developed initially by Friedman (1953), the Theory of Rational Choice (TRC) is based on a holistic approach and has achieved paradigmatic status in economic sciences. More specifically, the TRC states that individuals act according to two criteria: maximization and coherence, in which rationality is a link between information and individual preference. While this theory helps predict expected decision results, some authors (Elster & Gerschenfeld 1986; Bourdon 2004; Allais 1955) highlight its lack of realism. TRC does not in fact take account of environmental factors, or of the subjects' experiences and intuition, and thus has certain inherent limitations.

In response to these, Kahneman and Tversky (1977) developed a decision model that departs from the theory of rational choice and attempts to define the mechanisms leading to individual and collective decision-making. Basing their theory on a heuristic approach that privileged heuristics and biases (HB), Kahneman and Tversky proposed decision-making as the product of mechanisms of interaction between the automatic system and the reflected system. In HB, mental process is constituted by two different systems: the automatic system (System I) based on immediately available knowledge, always able to generate an answer,

and the reflexive system (System II) producing judgments and able to rationalize the ideas produced by System I.

More concretely, System I is based on innate abilities and makes quick associations between ideas (Morewedge & Kahneman 2010). It is known for translating emotion into impulsion, given that emotion is understood as a psychological and physical reaction to a situation. As such, System I may lead individuals to act suddenly (by reflex) without thinking about the consequence (Baratt 1993). System II uses memory and requires attention and effort to work (Beatty & Kahneman 1966; Kahneman, Tursky, Shapiro, & Crider 1969). Consequently, when this system is called into play, it becomes difficult for the individual to perform multiple actions at once (Kahneman 2012). In practice, System I generates suggestions (feelings or intuitions) when a new situation arises and submits them to System II, which decides to launch actions. But the two systems may conflict (Gilovich, Griffin, & Kahneman, 2002). In this case, automatic reaction coupled with the intention of correcting a situation may cause problems.

As to our subject of interest, cyber operations may attempt to change System I in order to produce unexpected behavior in the targeted organization's agents. Effectively, changing System I will generate biased suggestions and result in a change of actions triggered by System II based on System I data. Moreover, intuition—managed by System I—comes from emotions and thus from the affective domain. Here, military values may switch from cognitive to affective and be reinforced by individual experience, modifying the intuition. According to Klein (1999) intuition also comes from experience, and military personnel usually develop strong intuition in their own field of action. According to Kahneman's theory, the efficiency of cyber operation as described could be particularly important.

As such, this study examines the possibility that cognitive-dissonance-based psyops can change both soldiers' trust and behavior, as we will see in the presentation of data and analysis. Failure of frontline soldiers to carry out orders properly could endanger an entire operation. To cause this, cognitive dissonance must change a soldier's trust and decision-making. Accordingly, prior to proceeding we must look at the literature on trust and cohesion in military affairs.

Trust and Cohesion in Military Affairs

Trust seems to be the cornerstone of military cohesion and performance. According to McAllister (1995), trust has cognitive and affective underpinnings and is a factor of cohesion. Some meta-analytic studies show a positive relationship between cohesion and performance (Mullen & Cooper 1994). In military matters, performance means achieving the goal of a successful mission with as little loss as possible. Other sources propose three main components of military cohesion: relations between peers, relations between superiors and subordinates, and relations between the armed forces and the government (Stewart 1988; Etzioni 1961). Hence for soldiers, degrading the perception of government and increasing mistrust in superiors will deteriorate cohesion and performance, increasing the risk factor in mission success.

While trust is primordial, it remains a nebulous concept that needs clarifying. Bhattacharya et al. define it as "the expectancy of positive outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty" (Bhattacharya et al. 1998). Another definition from Rousseau et al. (1998) indicates a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another. Lastly, Mayer, Davis, and Schoorman (1995) define trust as "a willingness to be vulnerable to another party when that party cannot be controlled or monitored." These definitions are particularly apt here because our subjects

live and act under extreme situations. Accepting vulnerability is very real in that they can be wounded or even die in action.

Previous definitions of trust described uncertainty as a game changer. For Rivolier (1998), extreme situations are fast-changing with high levels of uncertainty for participants. To be considered extreme, a situation must also be risky (Lièvre 2014). In military parlance, vulnerability is a recurrent keyword in the definition of trust. Given that soldiers operate in extremely risky situations, it seems clear that trust is a cornerstone in achieving their tasks. In the event of failure, over and above their own mission is the government's credibility and trustworthiness. This can be diminished in its citizens' eyes (if soldiers come home wounded or die in battle, for example) and possibly its allies' too. So, eroding the trust of soldiers may have considerable effects not only on the battlefield but also on the government's policy and stability.

Cyber Operations, Access to Information, and Changes in Trust

Finally, in terms of literature review, in the case of Ukraine, the target of cyber operations was information. Based on our observation of increased uncertainty resulting from cyber operations, a comprehensive update on research into this issue seems appropriate.

According to Negroponte (1995), we live in a digital world, and military personnel are no exception: they are as connected as anybody else. Many of the soldiers we surveyed are "Generation Y;"[2] judging by Internet and mobile data consumption figures, this generation is among the most highly connected in history. A survey conducted by Omnibus Institute in the United Kingdom showed that 18 to 34-year-olds look at their smartphone up to 100 times a day, in other words every 9 minutes and 50 seconds. The growth of smartphones has caused a major shift in how we inform ourselves. As far as social media consumption is concerned, mobile usage grew by 30 percent from 2015 to 2016, an increase

[2] *Generation X* refers to people born between 1966–1976; *Generation Y*, or Echo Boomers or Millennials, to people born between 1977–1994; *Generation Z* to people born between 1995–2012.

of 581 million. Over 91 percent of the 2.8 billion people on social media are connected via mobile devices, and soldiers are no different.

Cyberspace, being a vector of information, changes how people inform themselves, and therefore influences their trust. Although information access may vary depending on age, the trend is clear: more and more people use the Internet to get information, many through social networks. Only two soldiers in our sample were not connected to social networks. So, people can easily be targeted in cyberspace by "information" created for the need of a psyops strategy using cognitive processes. Given that all the soldiers interviewed owned smartphones and said they use them for surfing the web and social networks, analyzing the trust attributed to web-sourced information seems important in understanding how it can be used by an adversary to influence soldiers' perceptions. According to the American Press Institute and the Associated Press-NORC Center for Public Affairs Research (2016), the person sharing a post was considered more important than the original source of information. The survey results showed that the individual sharing the information had a major effect on how trustworthy the information was considered: 51 percent of people said an article was well-reported when shared by a person they trust. With Facebook, 48 percent of the interviewees said how much they trusted the person posting the article influenced how much they trusted the information in question.

As to the military, given the special training and resulting team spirit, we postulated that if information is posted by a soldier, or someone sharing the same values (volunteer, etc.), a soldier's trust in the content will increase. The analysis of data in Part II vindicate this.

The Case of Ukraine

Ukraine has been facing the biggest deployment of cyber operations against a country ever seen. In light of the literature presented in Part I, we examined the possibility that the

trust of active and veteran Ukrainian soldiers had been affected by cognitive methods of Internet-based attacks. The purpose was to see whether their perceptions had altered and uncertainty increased in relation to their Internet consumption, and if so whether the effect was significant enough to modify their behavior. Another key question was whether they were aware of being potential targets or not.

Significance of the Case Study

Before answering these questions by means of data analysis, we discuss the value of Ukraine as an example. In Ukraine, the kinetic conflict was accompanied by massive waves of cyberattacks of many kinds. While Russia had already used such methods against Estonia and Georgia, the case of Ukraine is unprecedented in its magnitude. For many experts (Greenberger 2017; Weedon, 2015), it was a blueprint for testing various methods and estimating their effects. For NATO's CCDCOE, the use of cyberattacks by (in all appearance, Russia) was part of a broader strategy of information warfare (Geers et al. 2015).

Specific to Ukraine, cyberattacks included psyops cyber operations intended to affect as many people as possible and weaken the central government and country. We found that various channels were used in order to match the psychological profiles of targets and that the military was no exception, quite the contrary. Many military personnel received text messages on their mobile phones, encouraging them to stop fighting, go back home, or leave their positions. Meanwhile, more subtle operations were conducted through the Internet. We found that the soldiers we interviewed had received fraudulent messages. For example, the profiles of dead soldiers were used to send Facebook chat messages and spread "information" to sow doubt and mistrust toward state institutions. The soldiers explained that since they didn't know their "brothers in arms" were actually dead they were more inclined to believe these messages. This is paramount as such operations used soldiers' in peer-group trust to sow doubt about members of government or commanding officers.

Active fighters were not the only targets: a vast operation was also conducted on veterans. Veterans are ideal targets, as they exemplify an ideal of heroism for the general population, occupy a special position as thought leaders or national symbols, and have been trained in firearms handling. Many of them are young and thus part of the labor force and have political weight as voters and/or potential political leaders. Moreover, their past in EO makes them a potentially explosive social group. The way they feel can therefore have a profound influence on people's perceptions.

Except for certain occasions—tactical war phases, for example—the final goal seems to be to increase uncertainty in the minds of soldiers and fighters. To this end, some information media such as blogs or social networks were used (Weedon 2015). These practices are in accordance with Russian cyber warfare strategy such as developed by General Gareev (2015), or Colonel Chekinov and Lieutenant General Bogdanov (2011, 2013). According to them, information is a component of New-Generation War (NGW). As such, subversive operations involving information can be used to create chaos and provoke various kinds of disturbance, including weakened state resilience. Russian cyber warfare strategists have even recommended the use of mass media to stir up chaos and confusion in government but also in military management, particularly command and control. This matches the desired results of operations conducted in Ukraine. As a mirror effect, their recommendations for safeguarding Russia from such operations can be reversed for devising battle plans. For instance, their proposals included keeping sources of domestic (Russian) information out of reach of adversarial influence; yet in Ukraine, information channels were penetrated by exogenous influence.

Last but not least, Russian cyber warfare strategists have advised that information, including psychological warfare, should predominate in NGW, and be used extensively. The effect on the human psyche targeted is clearly to misinform, as well as encourage discontent

and unlawful acts. Analysis of the data collected in Ukraine thus seems to suggest a global military strategy, since loss of trust resulting in disengagement and changes to soldiers' behavior can be assimilated with unlawful acts based on discontent. Further, the result of these operations upon the execution of orders is clearly disruptive of military management, and command and control.

Data Collection and Research Methodology

Since 2014, we have made several trips to Ukraine, during which we witnessed cyber operations on various population levels. The data collection presented is based on research into the literature and field observations, static and dynamic, on and off the battlefield.

The goal of the research trip in February 2017, during the battle of Avdiivka, was to interview soldiers and veterans and establish whether their uncertainty had changed according to their Internet consumption, specifically according to a certain type of content. For context, the government had been vigorously promoting military values since the beginning of the conflict in Ukraine. Travel was initially planned to Avdiivka. However, due to the battle that broke out in the city, safe access was not assured, and we traveled instead to Poltava and Krementchuk. Poltava has a hospital where many wounded soldiers were treated for physical and psychological trauma. Krementchuk has a military school and a large part of its population was affected by the war. In addition, many soldiers were based in these cities to ensure turnover on the front line, ensuring ease of access to interview subjects.

Survey methodology

After local contacts had introduced the researchers to various groups, thirty active soldiers and veterans were interviewed after being divided into two groups, one of fifteen veterans (all wounded physically or psychologically) and one of fifteen active soldiers. The soldiers were assured of their anonymity and that the interviews would be neither transmitted nor published, as much for reasons of national security as to increase their trust in the

researchers. The surveys used a qualitative approach designed to obtain as much information as possible.

Concerning the question set, the interviews were not strictly directed but many questions were recurrent, thus allowing an analytical framework to be defined. For instance, the soldiers were asked to quantify their trust in various structures (group, institution, and government) on a Likert scale from 0 to 5, as well as their confidence in various kinds of media (radio, television, social networks, and alternative media such as blogs and nongovernmental information websites). They were also invited to explain their Internet habits and how they get their information. They were surveyed on how they felt about their institution and government before and after operations and also asked about the various media they listen to and why. The subjects were thus interviewed to ascertain whether their trust and perception of the government and their military hierarchy could have been influenced by cyber content and/or their Internet consumption. Lastly, they were asked about their perception of being or not being a potential target for psyops on the Internet. They were asked to elaborate on their answers. The interviews were sometimes followed by discussions on Skype or by email at the soldiers' discretion. Several of them used these discussions to send material, especially fake profiles they had spotted, or blog posts that particularly interested, impressed, or influenced them.

Analysis and Results

The qualitative data were processed with Nvivo 12; some data were extracted using Excel in order to express results as percentages, allowing us to perform the analysis presented here.

Analysis of the data collected from interviews with soldiers in Ukraine sheds light on several points. First, their daily consumption of Internet data was very diverse (from 0.5 to 6 hours). Nonetheless, it seems that the ones who changed their mind the most were those

connected two to four hours per day, in other words it was not the biggest consumers who were the most influenced. However, we need to look more deeply into this observation, especially when it comes to the data consumption environment (private or public, etc.). Second, in terms of age, it seems that soldiers belonging to "Generation Y" were more responsive and increased their uncertainty level toward institutions and government most. Some of them went so far as to say they had changed their behavior enough to not strictly obey a direct order. As justification, they explained that they had discovered details revealing that some of their commanders were not as "trustworthy" as they expected them to be. One of them explained that "I won't risk my life for someone who shows no respect for us, the sons of Ukraine, and for our wounded." Here, we also noticed the development of a gap between "us" the soldiers, and "they," "the others," in other words, the military hierarchy or members of government.

The interviewed soldiers' experience and participation in kinetic operations seemed to give them the feeling that they were more legitimate than the government in judging the merit of an action. For instance, one explained, "I believe less and less in people who do not have their hands in grease, who had never been on the field;" another told us that "there are too many people talking about what they do not know ... it's getting on my nerves." Yet another soldier concluded that "they are wearing figures just for the pictures, reality is that they don't know anything." At the same time, one thing we observed in a focus group of Ukrainian soldiers was that they never stopped believing in the core of their cause ("fighting for Ukraine") but have gradually dissociated it from Ukraine's government. One explained, "I believe less and less in our government and its capacity to help us. I only believe in Ukraine, those who fight. Those who do not stop fighting."

Indeed, the growing mistrust of the "others" has ratcheted up doubt in their government and, for some, President Poroshenko in particular. As to their level of trust in

various media, they mainly seemed to trust social networks and alternative media more than official ones, which are perceived as tied too much to government or oligarchs. For instance, one explained to us that "the newspapers, the big media belong to men who serve politics, so it's not the truth that they want us to believe." Another said, "when you are not paid for your publication you are more honest, so I think blogs and social network lie less than big media."

In explaining this gap in trust, soldiers argued that they mostly trusted their brothers in arms" and volunteers because they had similar experiences and fought for the same cause. It also seemed quite clear that their self-perception was strongly linked to their soldier's identity (even if they had other professions before the war) and patriotic fight for their country. Furthermore, they described themselves using military values and vocabulary (like patriotism, honor, and loyalty). It seems that they adopted these cognitive data (learned by training, the very nature of their job) as part of themselves, of the way they perceive themselves: these cognitive elements have become personal and affective ones. The cognitive components of their training and conditioning eventually became part of their personality.

According to the research we conducted, the soldiers we interviewed and surveyed seem to have been targeted by multi-step operations. Firstly, strong cognitions inherited from training were reinforced. In a military environment, this was easy to achieve since the targets believed their contact (the writer of the papers they read or sharer of the information seen or heard, etc.) was involved in military operations and therefore shared the same values. This was indicated by the use of expressions such as "brother in arms," "sons of Ukraine," "we," or "us." Furthermore, since this concerns values of importance to soldiers, the agent involved appears increasingly trustworthy. Consequently, an adversary can send misinformation to his target, linking this cognition with the field in which he wants to sow doubt.

For instance, soldiers showed us articles associating a member of government or a superior with the disrespectful treatment of veterans or wounded fighters who, in a soldier's

belief system, deserve military honors. As the information is completely opposed to the way soldiers want to see themselves and their values, this content was rejected. This example is no exception, and this kind of reaction is founded on soldiers' self-perception, even if it is based on cognitions resulting from training and conditioning. We thus noticed that some soldiers' strong cognitions were reinforced, particularly via Internet chats with apparently fake profiles or through the fraudulent use of deceased soldiers' profiles. Other strong cognitions were increased through blogs forwarded by "friends" or by other soldiers, sometimes real but sometimes created on purpose.

Thanks to mobile data, interactions between the targets and psyops agents can occur every day. Some may encourage targeted persons to perform specific actions at specific times, but this is very unlikely. It would require the conjunction of two complicated phenomena: an exact action and an exact time. When the focus group was asked whether they thought they could be a target of interest, the answer was unanimously "no." The explanation given was that, in their opinion, they were not strategic targets because they were not officers and did not hold strategic information or data. They particularly did not feel they could be strategic targets themselves. On the other hand, the focus group agreed they could be targeted by propaganda, but as Ukrainians and not as soldiers. Were it to happen, however, they thought it wouldn't work on them as they "knew separatists' and Russian lies too well to be fooled." Yet, the focus group only referred to "higher" propaganda and not its most subtle forms, i.e., the use of cognitive dissonance. One counterintuitive result is that soldiers felt they were not affected by cyber operations, all the while acknowledging that their opinion about the government and military command had changed as they "learned" more about them, largely through information obtained online.

The implications here are important. If the perpetrator of an attack were to obtain an increase in uncertainty among a large enough proportion of a military team, this could

increase his ability to cause the operation to fail. With increased levels of doubt and uncertainty, military personnel may not behave as they are supposed to. This is very dangerous as mission planning is built on the basis that soldiers will obey orders without variation and relies on behavioral stability. In the end, the nature of behavioral change does not matter. What does is that overreaction could be as dangerous for the conduct of a mission as underreaction. By underreaction, we understand a weaker response than expected, such as not executing an order or taking more time to carry it. In all cases, targeted soldiers do not accord with their conditioning and engagement. It is this 'disengagement' that can jeopardize the mission. These operations and their observed effects are related to trust in military teams, and to military psychology. Using cyber operations could be particularly advantageous for an adversary. Their efficiency can be significant on two levels, first from a practical point of view, in other words, on efficiency, and second in terms of the interest to the organization using these kinds of operations, in other words, on strategy. Concerning efficiency, many people use the internet to get information, in other words, cognitive elements. Cognitive dissonance can thus be used to trigger a psychological motivational discomfort and attempt to change the behavior of any subject. In addition, the internet can be used all day long to affect people, which means they can be subjected to several phases of cognitive dissonances, thereby increasing the rate of success in behavior change. Moreover, in accordance with the theories of Aronson (1968, 1992, and 1999) and Cooper & Stone (1999), cognitive dissonance can be deployed if a target's training is known and the values learned have become part of their personality, as occurs in the military. The Ukrainian case seems to validate this theory.

Conclusion

Based on the above observations, it appears that cognitive dissonance through misinformation circulated on the internet can be used as an efficient tool for psyops to affect

trust. If Ukraine were indeed a blueprint for Russian destabilization operations, the methods used were presumably worked out beforehand. In agreement with the concept of cognitive dissonance, the more the cognitive and affective dimensions are merged, the easier it should be to influence somebody using methods discussed in this theory. In the case of soldiers, since training and personal values merge in accordance with self-consistency theory, an adversary can easily obtain the profile of a military team, including soldiers' self-perceptions. In other words, the more someone is trained and conditioned, the more he can become a target. This holds the possibility of many practical consequences.

First, using the training and conditioning of military personnel as key component of these cyber operations, the assailant does not need to send agents into the field, close to targets, to perform individual psychological profiles. It is not only safer, decreasing the risk of being unmasked, but also less expansive, as long as the training and values inculcated have been studied enough. Looked at cynically, using this method, part of the work is done by the victim, not by the assailant, thereby reducing the latter's work. Further, as the target changes his behavior in accordance with the values he believes in and the training he received, he will not realize he is acting under someone else's influence. In our study, soldiers stated they couldn't be targeted and, even if they were, wouldn't be affected. Finally, we may suspect that when a soldier is subject to long-term cognitive dissonance, even if he does not change his behavior, he will feel psychological discomfort, for cognitive dissonance affects brain activity, in particular the prefrontal cortex and anterior cingular cortex (Gehring et al, 1993; Amodio, et al, 2004; Harmon-Jones et al, 2008). This in turn becomes a human management issue during both the short and long terms for the assaulted person. On the strategic level, the benefit of this kind of weaponization means that it will be very complicated to prove the involvement of the head of operations, and just as complicated to detect the attack itself. In the Ukrainian case, even if president Poroshenko points the finger at Russia for many of the

cyber-attacks and cyber operations his country has faced since 2014, actually proving Russian involvement is very complicated. Given the wide range of people and events involved, it would be very difficult to link attacks conducted via multiple channels with an overall state strategy. Concerning Ukraine, various hacker groups are known to be involved in the war, such as CyberBerkuts, Cozy Bears, FancyBears, or SandWorm. However, despite strong suspicion, no sufficient proof has ever been brought to a court of law. Consequently, any government might find it useful to hide behind seemingly autonomous hacker groups to target another country without fear of falling under the scope of international law, military or otherwise. Alternatively, those attacked can hardly respond in kind if they wish to respect the law.

Further, since either detecting or attributing these cyber operations is complicated, assailants could more than likely apply them during peacetime. The high level of internet penetration and the fact that cyber's multi-channel nature can be used to generate cognitive dissonance and affect System I enough to upset its relation with System II is extremely interesting, particularly because no commitment is needed for the outbreak of information dissonance (Vaidis and Gosling; 2011). Thus, if information that appeared on a smartphone can trigger dissonance, the target does not need to have sought the information for a reaction to be emulated. Moreover, the rapid growth of 5G will probably play its role in future developments, revolutionizing our relationship with technology and information. As such, the present results are probably just the first step in further research, as operations like this are likely to increase in importance as time progresses.

Bibliography

Adams, B., Webb, R., Trust development in small teams, Defense research and development Canada, Toronto contract report, CR-2003-016, Guelph, Ontario; Human System Incorporated, 2003.

Allais, M., Fondements d'une theorie positive des choix comportant un risque et critique des postulats et axioms de l'école americaine. Paris: Imprimerie Nationale, 1955.

Amodio, D., Harmon-Jones, E., Devine, P.J., Curtin J.J., Hatley S., & Covert A., 'Neural signal for the detection of unintentional race bias', Psychological Science, 2004, pp. 85-93.

American Press Institute and the Associated Press-NORC Center for Public Affairs Research, 'Who shared it?' : How Americans decide what news to trust on social media, American Press Institute, 2017.

Aronson, E., 'The cognitive and behavioral consequences of the confirmation and disconfirmation of expectations', Application for research grant submitted to the National Science Foundation, 1968, Harvard University.

Aronson, E., The return of the repressed: dissonance theory makes a comeback, Psychological inquiry, 1999, pp. 303-311.

Barratt, E.S., Impulsivity: Integrating cognitive, behavioral, biological, and environmental data in W. G. McCown, J. L. Johnson, & M. B. Shure (Eds.), The impulsive client: Theory, research, and treatment, 1993, pp. 39-56. Washington, DC, US: American Psychological Association.

Battacharya, R., Devinney, T.M., Pillutla, M.M., A formal model of trust based on outcomes, Academy of management review, 1998, 23(3), pp. 459-472.

Bourdon, R., Theorie du choix rationel ou individualisme méthodologique? Revue du MAUSS, 2004, 2, pp. 281-309.

Cabinet Deloitte, Usages Mobiles 2015: A Game of Phones, annual report, January 2016

Chekinov, S.G, Bogdanov, S.A, "The Nature and Content of a New-Generation War," Voennaya Mysl' (Military Thought), 2013, No. 10, pp. 13-25.

Clarke, A.R., Cyber War, Harper Collins, 2010.

U.S DoD, JP1-02: Department of Defense Dictionary of Military and Associated Terms, DoD, Washington: DoD., 2010. https://fas.org/irp/doddir/dod/jpl_o2.pdf.

Elster, J., Gerschenfeld, A. Le laboureur et ses enfants: deux essais sur les limites de la rationalité. Paris: Les Editions de Minuit, 1986.

Etzoni, A., A Comparative Analysis of Complex Organizations on Power, Involvement, and their Correlates, The free press, New York, 1961.

Eurostat statistics explained. internet activities in the past three months by age group EU-28, 2016, Eurostat edition, 2016. http://ec.europa.eu/eurostat/statisticsexplained/index.php.

Festinger, L., Une théorie de dissonance cognitive, Les classiques de sciences usines et sociales, Paris, Enrick B Editions, 1956.

Friedman M., The methodology of positive economics, *in* Friedman, M., *Essays on Positive Economics*, Chicago, University of Chicago Press, 1953

Gareev, M.A (unattributed report summarizing his speech), "How Does One Develop a Modern Army?" Krasnaya Zvezda Online, 2016, 11

Geers, K., Giles, K., Wirtz, J.J., Lewis, J.A, Lebicki, M., Koval, N., Pakharenko, G., Weedo, J., et al, Cyber War in Perspective: Russian Aggression against Ukraine, CCDCOE, 2015

Gehring, W.J., Goss, B., Coles, M.G.H., Meyer, D.E., & Donchin, E., A neural system for error detection and compensation, Psychological Science, 1993, pp. 385-390

Gilovich, T., Griffin, D., & Kahneman, D., Heuristic and biases: the psychology of intuitive judgement, New York, NY, US: Cambridge University Press. 2002

Greenberg, A., Hunting the hackers: How Ukraine became Russia's test lab for cyberwar, Wired, (20 June 2017)

Harmon-Jones, E., Brehm, J., Greenberger, J., Simon, L. & Nelson, D., 'Evidence that the production of aversive consequence is not necessary to create cognitive dissonance', Journal of Personality and Social Psychology, 1996, pp. 5-16

Harmon-Jones, E., Harmon-Jones, C., Fearn, M., Singleton, J.D., & Johnson, P. 'Left prefrontal cortical activation and spreading of alternatives: tests of the action-based model dissonance', Journal of personality and social science, 2008, pp. 1-15

Hootsuite & We are Social, Special Reports Digital in 2017: Global overview, January 2017. https://wearesocial.com/special-reports/digital-in-2017-global-overview.

Jonas, E., Greenberg, J., Frey, D. Connecting terror management and dissonance theory: evidence that mortality salience increases the preference for supporting information after decision', Personality and social psychology Bulletin, 2003, pp. 1181-1189.

Kahneman, D., & Tversky, A. (1977). Intuitive prediction: Biases and corrective procedures. DTIC Document. Retrieved December 3, 2016.

Kahneman, D., & Tversky, A. (1981). The simulation heuristic. DTIC Document. Retrieved December 8, 2016.

Kahneman, D., Beatty, J., Pupil diameter and load memory, Science, 1966, vol 154, pp. 1583-1585.

Kahneman, D., Tursky, B., Shapiro, D., Crider, A., Pupillary, heart rate, and skin resistance changes during a mental task, Journal of Experimental Psychology, 1969, 79, pp. 164-167.

Klein, G.A., Source of Power: How People Make Decisions. Cambridge, Mass: MIT press, 1999.

Kulpin, A., Rauscher, K.F., Yaschenko, V., for East-West Institute, 2014, Critical

Terminology Foundations 2, In: Russia-US Bilateral on Cybersecurity, Habes B. Godwin III (eds), Policy Report 2/2014.

Libicki, M., Cyberdeterrence and Cyberwar, RAND Corporation, 2009.

Lièvre, P., Repères pour un management des situations extrêmes, 25e congrès de l'Association francophone de Gestion des ressources humaines, 6 & 7 November 2014.

McAllister, D.J., Affect- and cognition-based trust as foundation for interpersonal cooperation in organizations, Academy of Management Journal, 1995, pp. 24-95.

Mayer, R.C., Davis, J.H., and Schoorman, F.D., 'An Integrative Model of Organizational Trust', the Academy of Management Review, 1995, Vol. 20, No. 3, pp. 709-734

Morewedge, C.K., Kahneman, D., Associative processes in intuitive judgement, Trends in cognitive science, 2010, vol 14, Issue 10, pp. 435-440.

Mullen, B., Cooper, C., 'The relation between group cohesiveness and performance: An integration', Psychological Bulletin, 1994, pp. 210-227.

Negroponte, N., Being Digital, Alfred A Knops, New York 1995.

Orléan, A., Hétérodoxie et incertitude, Epistémologie et Autonomie, Les cahiers du CREA Ecole Polytechnique, 1986, Paris.

Rivolier, J., Stress et situation extrêmes, Bulletins de la psychologie, 1998, pp. 6-20.

Rousseau, D., Sikins, S., Burt, R., and Camerer, C.F., 'Not so different after all: a cross discipline view of trust', Academy of management review, 1998, 23(3), pp. 393-404.

Schaap, A.J., 'Cyber warfare operations: development and use under international law', Air Force Law Review n°64, 2009, pp. 121-170.

Stewart, N.K., The south Atlantic conflict of 1982. A case study on military cohesion, U.S Army Alexandria, 1998.

Stone, J., Cooper, J., A self-standards model of cognitive dissonance, Journal of

Experimental Social Psychology, 1999, pp. 228-243.

Vaidis, D., Gosling, P., 'Is commitment necessary for the arousal of information dissonance?', Revue Internationale de Psychologie Sociale, 2011, n°23, pp. 33-63.

Weedon, J., Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine, Chapter 8 In: Kenneth Geers (ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE Publications, Tallinn, 2015.