FOREIGN POLICY RESEARCH INSTITUTE

E-NOTES

"A nation must think before it acts." - Robert Strausz-Hupé

FEBRUARY 2015

RUSSIA'S USE OF DISINFORMATION IN THE UKRAINE CONFLICT

By John R. Haines

John R. Haines is a Senior Fellow and Trustee of the Foreign Policy Research Institute and directs the Princeton Committee of FPRI. Much of his current research is focused on Russia and its near abroad, with a special interest in nationalist and separatist movements. He is also the chief executive officer of a private sector corporation that develops nuclear detection and nuclear counterterrorism technologies.

All warfare is based on deception...To subdue the enemy without fighting is the acme of skill.
--Sun Tzu

We will not forget! We will not forgive!
--CyberBerkut motto

In the vanguard of the non-linear war now raging in eastern Ukraine is an old weapon, *disinformation*, wielded by an unconventional force. Exemplifying that force is the hacktivist group, *CyberBerkut*. It recently issued an ultimatum to Ukrainian President Petro Poroshenko to end the war in eastern Ukraine that "has plunged the people of Ukraine into an abyss of war, poverty, unemployment and despair."[1] It directed an additional threat to Prime Minister Arseniy Yatsenyuk:

> "Mr. Yatsenyuk! We start the countdown. You have three days to stop what you started. In the event our conditions are not met, we will open the world's eyes to all that is happening in the country. Personal correspondence top officials, telephone calls, secret documents — everything that we found by hacking the computers of employees of Ukraine's Security Service. You decide: to stop the bloodshed in your own country and start over from scratch, or to commit public suicide in front of millions of people."[2]

The newest fulfillment of this threat is the release of a set of documents CyberBerkut alleges it obtained by "cracking"[3] Ukrainian Defense Ministry computers.[4] The documents, published on CyberBerkut's website and the Russian portal LifeNews, purport to be correspondence between Ukraine's Deputy Defense Secretary, Peter Mehedi, and a senior Syrian

---

[1] http://www.cyber-berkut.org

[2] "Яценюку дали три дня для прекращения войны" ("Yatsenyuk given three days to end the war"). *Pravda.ru* [online Russian edition, 30 January 2015]. http://m.pravda.ru/news/world/formerussr/ukraine/30-01-2015/1246317-kiberberkut-0/. Last accessed 1 February 2015.

[3] *Cracking* is so-called "black hat" malicious hacking, the intention of which is to circumvent or break security measures.

[4] "Украина тайно продает оружие США в Сирию" ("Ukraine is secretly selling United States arms in Syria"). *LifeNews* [online Russian edition, 6 February 2015]. http://lifenews.ru/mobile/news/149465. Last accessed 6 February 2015. This is not the first time LifeNews has been the conduit for what is widely considered Russian government-sourced disinformation: in April 2014, it reported that the widely-discredited allegation that the business card of Right Sector leader Dmytro Yarosh was found at the scene of a deadly shootout at a separatist checkpoint in Slovyansk in eastern Ukraine.

commander, Brigadier General Talal Makhlouf.[5] If the documents are to be believed, they suggest American arms shipments intended for frontline units in eastern Ukraine were diverted by Ukrainian government officials and sold illegally for private financial gain to the Assad regime.[6]

Risible as this claim may seem, it is impossible to disprove on the basis of open-source evidence, but then again, that misses the point. The objective of disinformation, to borrow from Whitehead, is to impose a pattern on experience. It is a lens used to distort and pervert our understanding of facts. It is telling Ukrainians that their government is corrupt and has betrayed the forces fighting in eastern Ukraine. It reinforces the narrative among the "Territorial Defense Battalion" paramilitaries — for example, the "cyborgs" of the Azov Battalion whose defense of the Donetsk Airport lasted longer than the siege or Stalingrad or Moscow — that they are being sacrificed in the war, a common and recurring social media theme.[7] It provokes demoralizing backlashes — a 2 February protest on Kyev's Independence Square included calls for the imposition of martial law and the dismissal of senior defense and security officials — that are reported gleefully in Russian news portals.[8]

Americans and Western Europeans are not the intended audience for Russian disinformation about Ukraine. Instead, Ukrainians are: the intent is, at the minimum, to demoralize; and at the maximum, to provoke a popular backlash against the Ukrainian government, even a *putsch*. It is intended to sustain a narrative that the political leadership has abandoned the frontline forces fighting in eastern Ukraine, especially among army conscripts and nationalist paramilitary volunteer units. The purported Mahedi-Makhlouf correspondence is a variation on the *Dolchstoßlegende,*[9] the mythical "stab-in-the-back" of the army by craven politicians, exemplifying the corrosive effect of even less-than-artful disinformation.

This, then, is the less-noticed side of the conflict in eastern Ukraine. Bringing incidents of disinformation to light for discussion purposes can have risks since disinformation thrives on repetition. It is nonetheless important to understand the instrumental effect of Russian disinformation on eroding Ukrainians' confidence in their civil institutions and creating fertile ground for extremist groups on all sides.

A Non-Linear War[10]

Vladislav Surkov's use of the term *non-linear war*[11] exemplifies how Russian theorists characterize 21st century warfare. He wrote, "The old wars of the 19th and 20th centuries involved two sides. Now, it is all against all." Valery Gerasimov expands the term with a distinctly Russian view of modern warfare (with echoes of eastern Ukraine):

---

[5] Makhlouf (sometimes translated as "Makhluf") is the cousin of Syrian President Bashar al-Assad and commands the 103rd Brigade of the Syrian Republican Guard.

[6] According to one of the documents, these arms allegedly consisted of rifles, mortars, MANPADS, and night vision equipment.

[7] According to the Ukrainian news portal *Dzerkalo Tyzhnia* ("Mirror Weekly") Azov Battalion members who picketed the Ukrainian Defense Ministry on 30 January to demand it cancel plans to reorganize the battalion were denounced by Ukrainian Interior Minister Arsen Avakov, who wrote on his Facebook page, "Attempts to block the Defense Ministry of a country in wartime, especially during active frontline clashes is an act of treason." See: "Група бійців "Айдара" пікетує Міноборони, палять шини" ("Group of Aydar fighters picket Defense Ministry, burn tires"). Дзеркало тижня [online Ukrainian edition, 2 February 2015]. http://dt.ua/UKRAINE/grupa-biyciv-aydara-piketuye-minobroni-palyat-shini-translyaciya-163057_.html. Last accessed 6 February 2015.

[8] See: "Митингующие в Киеве попытались прорваться в здание администрации президента" ("Hundreds try to break into Ukraine president's office in Kyev"). *RT* [online Russian edition, 3 February 2015]. http://russian.rt.com/article/72220. Lasty accessed 7 February 20154. Also: "Far-right nationalist paramilitaries in Ukraine determined to make war, not peace." *ITAR-TASS* [online English edition, 3 February 2015]. http://itar-tass.com/en/opinions/775181. Last accessed 7 February 2015.

[9] The *Dolchstoßlegende* is based on the polemic of von Hindenburg, Ludendorff and others that the German army was "stabbed in the back" in 1918 by the civilian government. It was mythologized during the 1920s by the far right German National People's Party (*aka* the DNVP) and National Socialist German Workers' Party (*aka* the NSDAP) and used to vilify the so-called "November criminals" who signed the armistice.

[10] The concept of *linearity* is borrowed from mathematics in which there are two types, *systemic linearity* and *geometric linearity*. Systemic linearity exists where two conditions are satisfied, *proportionality* (outputs are proportional to inputs) and *additivity* (the whole is equal to the sum of its parts). Geometric linearity refers to the presence of clearly defined lines in geometric figures. Clausewitz used "chance" to describe systemic non-linearity in warfare that is caused by factors like fog and friction. Modern command and control systems have diminished systemic non-linearity; thus the emphasis has shifted to geometric non-linearity, the figurative "blurring of lines," where disinformation is a key method. It can be a figurative blurring where disinformation is used to create a false narrative around a conflict; or a literal one with deception by activity of false axes. For example, see two articles in *Voyennaya Mysl'* ("Military Thought"): Col. V.F. Shul'gin (1989). "Оперативнал Маскировка в современных условиях" ("Operational Maskirovka under Modern Conditions"). *Voyennaya Mysl'*. 6(1989), pp. 19-27. Col. A.D. Rublev (1991). "Создание группировок для проведения Первого контрнаступление" ("Establishing Force Groupings for the First Counter-Offensive'). *Voyennaya Mysl'*. 2(1991), pp.20-25.

[11] The term *non-linear war* is a construct of Vladislav Yuryevich Surkov former deputy chief of staff to President Vladimir Putin, who, until

> "A perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[12]

As Russians see it, all conflict is a means to a geopolitical end. Nonmilitary instruments — in one embodiment, the purposeful distortion of an adversary's sensibilities[13] — can rival the power of weapons in their effectiveness.[14] Peter Pomerantsev refers to this as "the weaponization of information."[15] For Gerasimov, "The information space opens wide asymmetrical possibilities for reducing the enemy's fighting potential."[16] The coordinated use of nonmilitary instruments to provoke civil unrest and instill fear to the point of panic last year in Crimea is a good illustration of the theory in action. The information space is the main battlefield in this conception of information warfare, "a battle between states involving only the use of information weapons in the sphere of information models."[17] It is, simply put, "to wage war without ever announcing it officially."[18]

What is "Disinformation"?

The English word "disinformation" is a translation of a Russian one, *dezinformatsia.* It involves a carefully constructed, intentionally deceptive message leaked by an operator who conceals his identity, either by hiding behind a cloak of anonymity or by acting indirectly through agent, witting or otherwise.[19]

An element of the Soviet-era concept of *maskirovka,* disinformation is the deliberate use of *misinformation* or misleading information.[20] In Shmuel Vaknin's deft description, it is "an open and authorized policy, a conscious decision to subvert language itself, to divert topology, to disinform, to transform reality into an inane hall of mirrors."[21] A former deputy chief of

---

he was forced out in May 2013, was known as one of the Kremlin's "grey cardinals." His first published use of the term was in his short story, *Bez neba* ("Without sky"), written under the pseudonym Natan Dubovitsky. The narrator is a child whose parents were killed in the war he describes in the story, one in which the narrator was brain damaged, and can now only see and understand things in two dimensions. See: "Без неба." *Честное пионерское* [online Russian edition, 12 March 2014]. http://www.ruspioner.ru/honest/m/single/4131. Last accessed 4 February 2014. The term "non-linear" [the conventional translation of the Russian word *ochagovyy* (очаговый)] appears in earlier discussion of Soviet and Russian military doctrine; for example, Major General V. G. Reznichenko's 1987 book *Tactics* (Moscow: Voenizdat).

[12] General Valery V. Gerasimov (2013). "Ценность Науки В Предвидении" ("The Predictive Value of Science"). *Военно-промышленный кур'ер* [online Russian edition, 5 March 2013] , p. 3. http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. Last accessed 4 February 2014. Gerasimov is Chief of the General Staff of the Armed Forces of Russia, and first Deputy Defense Minister. The *Voyenno-promyshlennyy kur'yer* ("Military-Industrial Courier") is a Russian language weekly newspaper.

[13] From V.F. Nikitchenko, et al., eds. (1972). *Kontrrazvedyvatel'nyi slovar'* ["Counterintelligence dictionary"]. (Moscow: Higher Red Banner School of the Committee of State Security under the Soviet of Ministers of the USSR in the name of F.E. Dzerzhinsky), p. 79. Nikitchenko was the KGB chief in Ukraine during the 1960s.

[14] For example, Major General Nikolay Turko, an instructor at the Russian Federation's General Staff Academy, writes: "The most dangerous manifestation in the tendency to rely on military power relates more to the possible impact of the use of reflexive control by the opposing side...than to the direct use of the means of armed combat." See: Alexsey A. Prokhozhev & Nikolay. I. Turko (1996). *Osnovy informatsionnoy voyny* ("Fundamentals of Information Warfare"). Report presented to the conference on "Systems Analysis on the Threshold of the 21st Century: Theory and Practice," Moscow, February 1996, p. 251.

[15] Peter Pomerantsev & Michael Weiss (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia.

[16] Gerasimov (2013), *op cit.*

[17] Sergei P. Rastorguyev (2002). *An Introduction to the Formal Theory of Information War* (Moscow: Vuzovskaya Kniga).

[18] Mark Galeotti, quoted in Pomerantsev & Weiss (2014), p. 29.

[19] *Ibid*., p. 52.

[20] *Maskirovka* (маскировка) translates in English as literally a "little masquerade," but the nuanced term means something more along the lines of deception and purposeful misdirection. James Hansen wrote in the Central Intelligence Agency's journal *Studies in Intelligence*, "Moscow has always had a flair for D&D [denial & deception], known in Russian as *maskirovka*. Its central tenet is to prevent an adversary from discovering Russian intentions by deceiving him about the nature, scope, and timing of an operation." [Hansen (2002). "Soviet Deception in the Cuban Missile Crisis." *Studies in Intelligence*. 64:1. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article06.html. Last accessed 2 February 2015]

[21] http://samvak.tripod.com/pp58.html.

the Czechoslovak ŠtB[22] analogized disinformation to poison, saying, "One drop may not be a problem, but together, a dose could be fatal."[23]

Active measures — a Soviet-era term for political warfare — were defined by a Russian naval officer term as:

> "A means of eliminating, distorting or stealing information for the purpose of obtaining necessary data after penetrating the security system; blocking of access to information by its legitimate users; and in the final account, disorganization of all means of society's life support, including the enemy military infrastructure."[24]

Naked active measures can come dangerously close to open war. It would constitute an overt act of state aggression were the Russian government to admit openly to hacking Ukrainian government networks and stealing official documents. The same would be true if the Russian government admitted openly to disseminating stolen or counterfeit documents. Disinformation allows Russia to direct active measures aimed a destabilizing Ukraine without having to take public ownership of those measures.

Feliks Dzerzhinskii[25] established a "special disinformation office" within the Soviet Union's State Police Directorate in 1923.[26] *Dezinformatsiya* first received institutional status in 1959 when the Soviet KGB established a special unit in its First Chief Directorate known as the "Department For Active Measures." Using the cryptonym "Department D" and operating under the direct authority of the Communist Party Central Committee, Department D specialized in black propaganda and disinformation.[27] It was from the start true to its description by Dzerzhinskii's deputy, Martin Latsis, as "a fighting organ...It does not judge, it strikes."[28]

Propagandistic disinformation strives to demoralize. A classic if simple method of Soviet propagandistic disinformation was to disseminate forge documents[29] which for effect, however, contained at least some genuine information: "Every disinformation message," wrote Ladislav Bittman, "must at least partially correspond to reality or generally accepted views."[30] The overall purpose is to damage the target — Ukraine's government — by playing on the audience's prejudices and biases — a widely held suspicion of corruption among public officials. This allows propagandistic disinformation to be effective even when it comes from a source that the audience finds dubious or unreliable.

Technopower

Suspicion often creates what it expects.
--C.S. Lewis

---

[22] The abbreviation ŠtB stands for *Státní bezpečnost* ("State Security"), which was the counter-intelligence (2nd Directorate) directorate of the Czechoslovak Interior Ministry.

[23] Ladislav Bittman, quoted in Alvin A. Snyder (1995). *Warriors of Disinformation: How Lies, Videotape, and the USIA Won the Cold War.* (New York: Arcade Publishing).

[24] Rafaėl' Rifgatovich Bikkenin (2003). "*Kontseptsii informatsionnoy konflikt v voyennoy sfere*" ("Concepts of Information Conflict in Military Sphere"). *Morskoy Sbornik* (Navy Journal). [Russian language edition, 8 September 2003]. 10 (October 2003), pp. 38-40. Foreign Broadcast Information Service Daily Reports FBIS-SOV, 6 February 2004.

[25] Feliks Edmonovich Dzerzhinskii was a Polish-born Bolshevik whom Lenin in 1917 appointed Commissar for Internal Affairs and head of the All-Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage. The latter was better known as the Cheka. a name derived from the Russian acronym (ЧК) of its abbreviated name, the "Extraordinary Commission". Russian. Russian: чрезвыча́йная коми́ссия (ЧК). Russian transl.: *Chrezvychaynaya Komissiya*. It was the predecessor to a long line of Soviet state security agencies including the NKVD and the KGB.

[26] The State Police Directorate was known as the GPU (*Gosudarstvennoye politicheskoye upravlenie*). It was part of the Soviet Union's internal security and intelligence service, the People's Commissariat for Internal Affairs, also known as the NKVD (*Narodnyy Komissariat Vnutrennikh Del*)

[27] Hans Graf Huyn (1984). "Webs of Soviet Disinformation." *Strategic Review.* XXI:4, p. 52.

[28] James Bunyan (1936). *Intervention, Civil War, and Communism in Russia: Documents and Materials, April-December 1918*. (Baltimore: Johns Hopkins Press), pp. 227, 261.

[29] Bittman (1985), *op cit.*, pp. 55-56.

[30] Ladislav Bittman (1985). *The KGB and Soviet Disinformation: An Insider's View.* (Washington, DC: Pergamon-Brassey's), p. 49. Bittman was the Deputy Chief of the 8th section of the 2nd Department of the Czechoslovak Interior Ministry until he defected to the West in 1968

Timothy Jordan conceptualizes *technopower* as a condition in which war no longer involves the conquest of new territory, but, rather, the destruction of the opponent's will to resist.[31] In the conflict in eastern Ukraine, *dezinformatsia* is a potent instrument of Russian technopower. It is a central component of what Russian theorists call *information warfare* (*aka* "information operations"), which is potentially one of the most damaging applications of force. Gerasimov described information operations as "military means of a concealed nature."[32] The aim is to manipulate information and exert psychological influences on another state's political and military leaders, soldiers, and civilian population.[33] Applied in Russia's near abroad, it is "information warfare as domestic counterinsurgency,"[34] something "capable of shaping public opinion to mobilize political forces against the authorities in their state."[35]

The creation and dissemination of disinformation in cyberspace is an important tactic in modern conflicts. Unlike the classic domains of military conflict (i.e., land, air, sea & space), cyberspace is not strictly speaking a domain. Rather, it is a built environment, which means it can be un-built and remodeled (and in the extreme, destroyed).[36] In the cyber frame of a broader cybered conflict, defensive information operations protect the integrity of electronic data. Their main function is to prevent "cracking" and other cyber attacks from successfully accessing, changing, and/or destroying electronic data, which might includes efforts to alter its context or otherwise manipulating it for purposes of deception.[37]

Cyberspace confers some distinct advantages on *dezinformatsia*: when dealing with electronic data or documents, neither style nor provenance (how it was obtained) is a reliable signal to indicate deception, unlike handwritten or typewritten material. An effective way to create disinformation with electronic data is to begin with a genuine message and then change some critical element (e.g., time, place, name) in a systematic way.[38] Disinformation created this way is easily disseminated through defaced governmental websites, which has the added benefit of confounding the adversary's information flows.[39]

Disinformation based on forged or altered electronic data is an important tool since governments rely on information and reputation to exercise moral influence and to model public opinion. Comingling strategic content (information that is genuine but compromising) and disinformation can alter a political balance and/or legitimate a broader conflict. It is an effective way to intervene in a target state's domestic affairs[40] that skirts the principle of international law that foreign agents cannot carry out activities within the territory of another state without its permission. As a practical matter, most states engaged in systematic campaigns to disseminate *dezinformatsia* do so in ways that makes its attribution difficult to prove.

From Asymmetric Warfare to Dissymmetric Warfare

Asymmetric warfare is a concept that is broad, inclusive, and as often as not, misapplied. It denotes where two sides in a conflict have such divergent strengths and weaknesses that they resort to drastically different — thus *asymmetric* — tactics to achieve relative advantage. The superior force in an asymmetric conflict will attempt to limit operations in order to keep its costs low. The inferior force will attempt to inflict the highest possible costs on its more powerful adversary, and to draw it into a war of attrition in which asymmetry favors the inferior force. One aim of asymmetric warfare is to make any countermove by the stronger force look like a significant and unwarranted escalation, which in the current conflict might be a pretense for deploying Russian "peacekeepers" into the territory.

---

[31] Tim Jordan (2002). "Technology and Its Cyberfutures." In John Armitage & Joanne Roberts, eds., *Living with Cyberspace: Technology and Society in the 21st Century*. (London: Continuum), pp. 120-131.

[32] Gerasimov (2013), *op cit.*

[33]Sergei Komov, Sergei Korotkov & Igor Dylevski (2007). "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law." In *ICTs and International Security* (Geneva: United Nations Institute for Disarmament Research), p. 36.

[34] Stephen Blank (2013). "Russian Information *Warfare as Domestic Counterinsurgency." American Foreign Policy Interests*. 35:1, pp. 31-44. http://www.tandfonline.com/doi/pdf/10.1080/10803920.2013.757946. Last accessed 5 February 2015.

[35] Russia Federal Security Service Information Security Center First Deputy Director Dmitri Frolov, quoted in Blank (2013), *op cit*., p. 35.

[36] Peter Dombrowski & Chris C. Demchak (2014). "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review*. 67:2, p. 75. They characterize cyberspace as a "substrate" or underlying layer on which modern society is built.

[37] William Hutchinson (2006). "Information Warfare and Deception." *Informing Science*. 9(2002), pp. 220-221. http://www.inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf. Last accessed 4 February 2015.

[38] Lech J. Janczewski & Andrew M. Colarik (2008). *Cyber Warfare and Cyber Terrorism*. (Hershey, PA: Information Science Reference), p. 100.

[39] *Ibid.*, xvi.

[40] For example, under the 1981 *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, it is "The duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States." See: United Nations General Assembly (1981). "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States." UN document A/RES/36/103 (9 December 1981), §II(j).

Asymmetrical actions, Gerasimov wrote, include informational ones: "The information space opens wide asymmetrical opportunities to reduce the enemy's fighting potential."[41] It is primarily a figurative war of narratives in which favorable ones are reinforced and multiplied while "foreign" interpretations are neutralized and pushed to the margins where they pose no threat.[42] Rastorguyev has long argued that defensive tactics in this kind of war would lead to defeat. Russia has accordingly reframed how it defines the threat in eastern Ukraine to fit an offensive war: the focus of Russian *dezinformatsia* is a purported rising anarchy in eastern Ukraine and the right of separatists to self-determination.

The opposite of asymmetric warfare is *dissymmetric warfare,* which results from the application of massive force against a weaker opponent in a military conflict. Ukraine confronts both asymmetric and dissymmetric dimensions in the war in eastern Ukraine. Pro-Russian separatists wage asymmetric warfare against the Ukrainian government — information warfare shares many features with classic guerrilla warfare, for example, the absence of a single frontline or a formal declaration of war — while Russia prosecutes a parallel, dissymmetric one.[43] The Ukrainian government has been unable to transform the asymmetric war against pro-Russian separatists into a dissymmetric one in which Ukraine could exploit its advantages. This reflects several factors. The separatist forces have demonstrated considerably higher esprit de corps than Ukraine's, whose regular army units are increasingly dependent upon conscripts[44] (thus Ukraine's risky gambit to "stiffen" army units by deploying ultra-nationalist paramilitary units to front line positions). Separatist forces also have limited their actions to waging a genuine asymmetric conflict that makes optimal use of terrain and keeps to guerrilla warfare tactics.

The dissymmetric war in eastern Ukraine (for the most part so far) is a cybered conflict. [45] Ukraine faces a determined, capable adversary — the Russian government — that is highly skilled in the use of *dezinformatsia* to impose virtual costs and virtual collateral damage, in this case on Ukraine. The hostile use of information and communication technologies (ICTs) is a Russian conceptualization meant to influence or damage an adversary-state's information resources and telecommunication systems. It includes disseminating disinformation and creating virtual depictions in cyberspace that misrepresents reality, all geared toward disorienting, destabilizing and demoralizing a civilian population.[46] Properly used, disinformation has an outsized "shock and awe" effect that saps an adversary's will to fight, largely by distorting how its civilians perceive and understand the conflict.[47] In the current one, cyberspace has becomes Ukraine's second ungovernable badland, one in which it is fighting an unconventional cybered war alongside the conventional one in the physical space of eastern Ukraine.

CyberBerkut & the Conflict in in Eastern Ukraine

The hacktivist group CyberBerkut[48] is the vanguard of a sophisticated *dezinformatsia* campaign in Ukraine. Since first emerging in March 2014, it has been implicated in multiple incidents of cyber espionage, including direct denial of service (DDoS)

---

[41] Gerasimov (2013), *op cit.*

[42] Jolanta Darczewska (2014). *The Information War on Ukraine: New Challenges*. Cicero Foundation Great Debate Papers No. 14/08 (December 2014), p. 9. http://www.cicerofoundation.org/lectures/Jolanta_Darczewska_Info_War_Ukraine.pdf. Last accessed 5 February 2015.

[43] Albert A. Stahel (2003). "Dissymmetric warfare versus asymmetric warfare." *International Transactions in Operational Research*. 11, p. 443.

[44] President Poroshenko on 14 January 2015 signed a decree ordering the mobilization of an additional 50,000 conscripts. The new mobilization — Ukraine's fourth since February 2014—will be occur in three phases in January, April, and June 2015. The Ukrainian parliament endorsed the presidential decree the following day, and raised the upper age limit for male citizens from 25 to 27 years, with recruits serving for 1.5 years. There has been notable resistance to the new mobilization: according to presidential adviser Yuri Birykov, 37% of new conscripts in western Ukraine's Ivano-Frankivsk region have left Ukraine. So, too, in the neighboring Chernivtsi region, where 17% of conscripts have crossed the border into Romania; and in the Lutsk and Rivne regions, where 19% of conscripts have refused military service on religious grounds. Conscripts wil be demobilized only after Ukraine reaches a durable truce in the eastern part of the country, according Poroshenko.

[45] *Cybered conflict* is a broader term than *cyber conflict*, which implies that the conflict remains exclusively within the domain of cyberspace. The conflict in eastern Ukraine, like many conflicts, involves many elements that are cyber-related but do not exist solely within cyberspace. A cybered conflict may have phases that are purely cyber; for example, a preparatory phase or a large-scale deception operation. See: Chris Demchak (2010). "Cybered Conflict vs. Cyber War." The Atlantic Council [online edition, 20 October 2010]. http://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war. Last accessed 2 February 2015.yber

[46] Anatolij A. Streltkov (2007). "International information security: description and legal aspects." In *ICTs and International Security* (Geneva: United Nations Institute for Disarmament Research), p. 7.

[47] Matthew T. Clements (2014. "Shock and awe: the effects of disinformation in military confrontation." *Policy Studies*. 35:3, pp. 211-220. http://www.tandfonline.com/doi/pdf/10.1080/01442872.2014.886679. Last accessed 30 January 2015.

[48] *CyberBerkut* is the Russian (КиберБеркут) and Ukrainian (КіберБеркут) transliteration of "Cyber Golden Eagles." The word *Berkut* ("Golden Eagles") is a reference to the symbol of a special police unit that existed within Ukraine's Interior Ministry. When the Yanukovych government fells in February 2014, one of the new government's first acts was to disband Berkut for its use of excessive violence against the Maidan protestors. Berkut was the successor to the Soviet-era Special Purpose Mobile Unit known by its Russian

attacks against NATO as well as Ukrainian and German government websites.[49] More recently, it has focused on the online publication of "cracked" or maliciously hacked electronic documents obtained from the computers of Ukrainian governmental and political figures.

The membership of CyberBerkut is anonymous, but reportedly includes former officers in the Crimean *Berkut*. That unit was part of Ukraine's Interior Ministry until Crimea's March 2014 annexation, upon which the Crimean *Berkut* was incorporated into Russia's Interior Ministry.[50] CyberBerkut's "Ukrainian identity" is vigorously asserted, however, as it postures as an internal opposition group. This, too, is consistent with the Russian playbook, for as Gerasimov wrote, "Asymmetrical actions...[include] internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions..."[51]

In the past several days, CyberBerkut published several sets of documents online that it claims were obtained from electronic records the group purportedly "cracked" from the Ukrainian Security Service, known as the SBU.[52] The first set of documents purport to show SBU complicity in a 13 January rocket attack in Volnovakha in which a civilian passenger bus was destroyed, killing 10 persons and injuring 17 (it is important to note that the circumstances of the rocket attack conflict with much of the "evidence" produced by CyberBerkut and others). One key document in this set purports to be a confidential letter from Vasili Gritsak to Hennadiy Kuznetsov[53] dated 13 January 2014. Gritsak is the SBU's First Deputy Chairman and the head of its Anti-Terrorism Center.[54] Kuznetsov, an SBU Colonel, at the time was head of Special Operations Center "A", a unit responsible for special anti-terrorist operations. The document contains what appear to be written directions from Gritsak directing Kuznetsov to carry out so-called "false flag"[55] attacks in eastern Ukraine's Donetsk and Lugansk regions. The objective, according to the document, is to produce civilian deaths that can be blamed on pro-Russian separatists. A companion document purports to be a report from the SBU Donetsk Regional Unit regarding its implementation of a propaganda campaign citing several media reports of the Volnovakha rocket attack.

Not surprisingly, similar documents have surfaced before. In December 2014, the online portal *Russiya Vesna*[56] ("Russian Spring") published a document on its website that it purported to be a 25 November order signed by Gritsak. In it, he directs

---

acronym, OMON [Russian: Отряд мобильный особого назначения (ОМОН). Russian transl.: *Otryad Mobilny Osobogo Naznacheniy*a (*OMON*)]. The unit was known for its distinctive blue urban camouflage or black uniforms and maroon berets.

[49] DDoS attacks work by flooding the target server with communications requests, so that it becomes unavailable for users. CyberBerkut claimed credit for DDoS attacks against NATO's main website (nato.int), its cyber defense center website (ccdcoe.org), and its parliamentary assembly website. (nato-pa.int). More recently, CyberBerkut claimed credit for a series of January 2015 attacks on German governmental websites, (including the German Chancellor and the Bundestag) timed to correspond with an official visit to Berlin by Ukrainian Prime Minister Arseniy Yatsenyuk.

[50] "Russian interior bodies created in Crimea and Sevastopol." *ITAR-TASS* [online English edition, 25 March 2014]. http://itar-tass.com/en/crimea-and-sevastopol/725269. Last accessed 2 February 2014. After Ukraine arrested former Berkut members who were accused of shooting Maidan protestor in February, Russia announced that ex-Berkut officers were eligible to receive Russian passports,

[51] Gerasimov (2013), *op cit.*

[52] The acronym is from the Ukrainian transliteration of the agency's name. Ukrainian: Служба Безпеки України (СБУ). Ukrainian transl.: *Sluzhba Bezpeky Ukrayiny* (*SBU*). The SBU is responsible for so-called "anti-terrorist operations" against separatist groups in eastern Ukraine on behalf of the Ukrainian government.

[53] On 23 January 2015 President Poroshenko issued a decree (No. 28/2015) dismissing Kuznetsov from his post. See: "Порошенко уволил начальника Центра спецопераций по борьбе с терроризмом" ("Poroshenko dismisses the head of the special operations center to combat terrorism"). *Обозреватель* [Ukrainian online edition, 23 January 2015]. http://obozrevatel.com/politics/74638-poroshenko-uvolil-nachalnika-antiterroristicheskogo-tsentra-sbu.htm. Last accessed 30 January 2015. Kuznetsov had been appointed to the post in March 2014 by acting Ukrainian president and parliament speaker Oleksandr Turchynov

[54] From the SBU website: "The Anti-Terrorist Center operating under the Security Service of Ukraine, deals with the organization and conduct of counterterrorism operations, as well as with the coordination of the activity of entities combating terrorism or engaged in counterterrorism operations." http://www.ssu.gov.ua/sbu/control/en/publish/article?art_id=83725&cat_id=83628. Last accessed 30 January 2015. President Poroshenko appointed Gritsov to these posts by on 7 July 2014.

[55] A false flag attack is an atrocity committed by military or security personnel that is blamed on terrorists. See: Geraint Hughes (2011). *The Military's Role in Counterterrorism: Example and Implications for Liberal Democracies*. (Carlisle, PA: U.S. Army War College), p. 105. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1066.pdf. Last accessed 30 January 2015.

[56] *Russiya Vesna* is a pro-Russian separatist website (rusvesna.su). The name is derived from a political theory developed by Aleksandr Dubin and published on his Facebook page in March 2014. [https://www.facebook.com/photo.php?fbid=747268065283236&set=a.147408498602532.29033.100000001479276&type=1&comment_id=3121437&offset=0&total_comments=3] Dugin's first scenario, the "Russian Spring", envisions the emergence of an anti-American confederation of the European Union and the Eurasian Union in the aftermath of Ukraine's collapse. Dugin posits two alternate scenarios, a "World War" between NATO and Russia; and "The Global *Maidan*" where American military pressure on Russia causes Putin's political

SBU units to execute false flag artillery attacks against several villages north of Donetsk, an area in which separatist units were known to operate. Afterwards, the document reads, the SBU will "organize visits to the villages by Ukrainian and foreign correspondents, who will be provided with evidence that 'terrorists' launched the artillery attacks."

On 28 January, CyberBerkut published another set of documents the group claimed are cracked electronic files belonging to Anatoly Matios, Ukraine's Deputy Prosecutor General and Chief Military Prosecutor.[57] The document that received the most attention orders an end to public reporting of the number of casualties suffered by Ukrainian forces "in the area of the ATO" (anti-terrorist operations) by hospitals under the jurisdiction of the Ukrainian Defense Ministry.

However, the most scandalous purports to be an order dated 25 January 2015 from Lieutenant-General Serhiy N. Popko,[58] who commands Ukrainian ATO forces in the Donetsk and Lugansk regions (and who currently is in the Debaltseve area). In it, he orders the formation of "protective detachments" comprised of members of "the volunteer corps," a reference to the Ukraine Volunteer Corps *aka* DUK-Right Sector, a paramilitary force organized by the ultra-nationalist political party Right Sector. The formation of protective detachments is intended "to prevent mass defections soldiers from the battlefield near Debaltseve."[59] The geographic reference is to a salient centered on the town of Debaltseve — a strategic railway hub connecting Donetsk and Lugansk — in which separatist forces are attempting to trap a force of several thousand Ukrainian soldiers and paramilitary. In a related document, Matios purportedly orders all personnel rotating out of the combat zone to first surrender their weapons.

A clear objective of the current *dezinformatsia* campaign being waged against the Ukrainian government is to exploit fissures: within Ukraine's coalition government; between the government and combatants in the field, especially the DUK-Right Sector and Azov Brigade paramilitaries; and between the Ukraine's regular army and paramilitaries. DUK-Right Sector leader Dmytro Yarosh[60] in late January threatened to split Ukraine's armed force by creating "a parallel General Staff...that would receive the support of many military units, both regular and volunteer." Shortly after Yarosh leveled the threat, the Ukrainian army's general staff announced its intention to disband all so-called "volunteer organizations" including the Aydar Battalion[61] and to "merge" them into other army units.

Within the past few days, the *dezinformatsia* campaign has taken direct aim at Yaros when CyberBerkut released documents that purportedly implicate him in a host of economic crimes:

> "Today we are publishing documents that expose the criminal activities of the head of Ukrainian neo-Nazis, which confirm multiple incidences of extortion – the illegal and cynical seizure of properties and businesses belonging to Ukrainian citizens by Yarosh and his associates. The stolen money is then taken out of the country through fronts and deposited in offshore accounts in Cyprus. Now everyone will know that the Ukrainian neo-Nazis led by Yarosh are common gangsters, and have used policies of the Maidan to cover up criminal activities and self-enrichment at the expense of the citizens of Ukraine."[62]

All this seems oriented toward driving a deeper wedge between Yarosh's Right Sector political allies — and the DUK-Right Sector paramilitary — and Ukrainians in and out of government who have long harbored suspicions about the proper place of far right ultranationalists in Ukraine's civil society.

---

demise and Russia's social collapse.

[57] The following day, Matios filed criminal charges against the leader of the group *Antivoyna* ("Anti-War"), Victoria Shilova. She is a former member of the Dnepropetrovsk Regional Council. *Antivoyna* has encouraged resistance to Ukraine's latest military mobilization, and Shilova was charged with "hindering the legitimate activities of military forces of Ukraine and other military formations."

[58] Interesting side note: In 2003, then Major-General Popko commanded a mechanized brigade in the Ukrainian peacekeeping force in Iraq that was part of Multinational Division Central-South.

[59] The quoted text reads in the original Russian: "В интересах предотвращения массового дезертирства военнослужащих с поля боя в районе Дебальцево."

[60] Dmytro Yarosh is the leader of the far right Ukrainian nationalist political party, Right Sector. In February 2014, he was appointed as deputy to Andriy Parubiy (who co-founded another Ukrainian nationalist political party, *Svoboda*) in his capacity as Secretary of the National Defense Committee, which supervises Ukraine's defense ministry and armed forces. In July 2014, Interpol fulfilled Russia's April 2014 request to issue an arrest warrant for Yarosh for "public incitement to terrorist and extremist activities involving the use of mass media." In January 2015, Yarosh was wounded in eastern Ukraine ehen he was struck by shrapnel.

[61] The Aidar Battalion, the first of many so-called Territorial Defense Battalions of Ukraine, is a volunteer military detachment within Ukraine's Defense Ministry.

[62] http://www.cyber-berkut.org. Last accessed 3 February 2015.

A Potent Fifth Column

War in general is not declared. It simply begins.
-- Georgii Samoilovich Isserson

It is a dubious suggestion that a field commander would commit an order to writing directing subordinates to commit what indisputably constitutes a war crime. That alone casts doubt on documents purporting to order false flag incidents against civilian populations. It is not, however, probative regarding all of the documents in question. It is certainly conceivable that military commanders would be reluctant to disclose casualty numbers in the midst of a mobilization and might direct that these statistics be withheld. As to alleged criminal acts committed by individuals associated with political parties that are part of the Ukrainian governing coalition (or regarding government-aligned paramilitaries), those claims are impossible to assess from the outside. Suffice it to say, however, that the bar should be high — far higher than allegedly cracked documents of dubious content and provenance — to seriously entertain taking such documents at face value. At the end of the day it is up to the Ukrainian people to decide.

There is no independent way to assess the status of the allegedly cracked documents released by groups like CyberBerkut or Russiya Vesna. It is possible some are genuine and mean what they say, but at the same time, genuine documents can be placed in a misleading context when bundled with altered or forged ones. It is also possible that some may be sourced from genuine documents but altered to create false meaning and to deceive. As to whether either is probable, the reader is left to decide.

There is no expectation that Russian *dezinformatsia* will lead to a groundswell of support for the pro-Russia separatists in eastern Ukraine. That is not the intent. It is to shape Ukrainian perceptions that the *Maidan* movement of just a year ago is a revolution betrayed. The intent is not to mobilize; it is to demoralize.

Vladislav Surkov's short story "Without Sky" concludes on a powerful note:

> "We organized a rebellion of the simple, the two-dimensional people against the complex and cunning. We are against those who never say 'yes' or 'no'. Who say neither 'black' nor 'white.' Who know the third word. There are many, many third words. Empty, false, confusing ways that darken the truth. These ways are the house of Satan. There, they make money and bombs, saying 'Here's money for the benefit of the honest, here's a bomb for the protection of love.' We begin tomorrow. We will win. Or lose. There is no third option."

The siren song of Russian disinformation notwithstanding, there is indeed no third option for Ukraine: it is either a sovereign nation or it is not. What is unresolved is whether a sovereign Ukraine will remain territorially intact, and whether democratic government will wither or flourish there. That is a struggle in which Russian *dezinformatsia* poses a potent fifth column.

FPRI, 1528 Walnut Street, Suite 610, Philadelphia, PA 19102-3684
For more information, contact Eli Gilman at 215-732-3774, ext. 103, email fpri@fpri.org, or visit us at www.fpri.org