The Ukraine List #485

compiled by Dominique Arel (darel@uottawa.ca)
Chair of Ukrainian Studies, U of Ottawa
www.chairukr.com
www.danyliwseminar.com

27 June 2017

For regular postings on Ukraine and Ukrainian Studies, follow me on Twitter at @darelasn

#1
Deadline Reminder: 28 June 2017

13th Annual Danyliw Research Seminar on Contemporary Ukraine
Chair of Ukrainian Studies, University of Ottawa, 16-18 November 2017
http://www.danyliwseminar.com

CALL FOR PAPER PROPOSALS

The Chair of Ukrainian Studies, with the support of the Wolodymyr George Danyliw Foundation, will be holding its 13th Annual Danyliw Research Seminar on Contemporary Ukraine at the University of Ottawa on 16-18 November 2017. Since 2005, the Danyliw Seminar has provided an annual platform for the presentation of some of the most influential academic research on Ukraine.

The Seminar invites proposals from scholars and doctoral students —in political science, anthropology, sociology, history, law, economics and related disciplines in the social sciences and humanities— on a broad variety of topics falling under thematic clusters, such as those suggested below:

Conflict
- war/violence (combatants, civilians in wartime, DNR/LNR, Maidan)
- security (conflict resolution, Minsk Accords, OSCE, NATO, Crimea)
- nationalism (Ukrainian, Russian, Soviet, historical, far right)

Reform
- economic change (energy, corruption, oligarchies, EU free trade, foreign aid)
- governance (rule of law, elections, regionalism)
- media (TV/digital, social media, information warfare, fake news)

Identity
- history/memory (World War II, Holodomor, Soviet period, interwar, imperial)
- language, ethnicity, nation (policies and practices)
- culture and politics (cinema, literature, music, performing arts, popular culture)

Society
- migration (IDPs, refugees, migrant workers, diasporas)
- social problems (reintegration of combatants, protests, welfare, gender, education)
- state/society (citizenship, civil society, collective action/protests, human rights)

The Seminar will also be featuring panels devoted to recent/new books touching on Ukraine, as well as the screening of new documentaries followed by a discussion with filmmakers. In 2016, four book panels (Lawrence Douglas/*The Right Wrong Man*, Catherine Gousseff/Échanger les peuples, Serhii Plokhy/*The Gates of Europe*, and Ioulia Shukan/*Génération Maidan*) were on the program and two films were screened (Elena Volochine/*Oleg's Choice*, Antony Butts/*DIY Country*). Information on the 2016 book panels and films can easily be accessed from the top menu of the web site. The 2017 Seminar is welcoming book panel proposals, as well as documentary proposals.

Presentations at the Seminar will be based on research papers (6,000-8,000 words) and will be made available, within hours after the panel discussions, in written and video format on the Seminar website and on social media. The Seminar will privilege intensive discussion, with relatively short presentations (12 minutes), comments by the moderator and an extensive Q&A with Seminar participants and assembled public.

People interested in presenting at the 2017 Danyliw Seminar are invited to submit a 500 word paper proposal and a 150 word biographical statement, by email attachment, to Dominique Arel, Chair of Ukrainian Studies, at darel@uottawa.ca AND chairukr@gmail.com.

Please also include your full coordinates (institutional affiliation, preferred postal address, email, phone, and Twitter account [if you have one]). If applicable, indicate your latest publication or, in the case of doctoral or post-doctoral applicants, the year when you entered a doctoral program, the title of your dissertation and year of (expected) completion.

Books published between 2016 and 2018 (as long as near-final proofs are available prior to the Seminar) are eligible for consideration as a book panel proposal. The proposal must include a 500 word abstract of the book, as well as the 150 word bio and full coordinates.

Films produced between 2015 and 2017 are eligible for consideration as a documentary proposal. The proposal must include a 500 word abstract of the film, as well as the 150 word bio, full coordinates, and a secure web link to the film.

In addition to scholars and doctoral students, policy analysts, practitioners from non-governmental and international organizations, journalists, and artists are also welcome to send a proposal.

The proposal deadline is 28 June 2017. The Chair will cover the travel and accommodation expenses of applicants whose proposal is accepted by the Seminar. The proposals will be reviewed by an international selection committee and applicants will be notified in the course of the summer.

To celebrate the 10th Anniversary of the Danyliw Seminar in 2014, a special website was created at www.danyliwseminar.com. The site contains the programs, papers, videos of presentations and photographs of the last three seminars (2014-2016). To access the abstracts, papers and videos of the 2016 presenters, click on "Participants" in the menu and then click on the individual names of participants. The 2016 Program can be accessed at https://www.danyliwseminar.com/program-2016.

Check the “Danyliw Seminar” Facebook page at http://bit.ly/2rssSHk.

For information on the Chair of Ukrainian Studies, go to http://bit.ly/2r7Hl8L.

The Seminar is made possible by the generous commitment of the Wolodymyr George Danyliw Foundation to the pursuit of excellence in the study of contemporary Ukraine.

#2
Kule Doctoral Scholarships on Ukraine

Chair of Ukrainian Studies, University of Ottawa
Application Deadline: 1 February 2018 (International & Canadian Students)

The Chair of Ukrainian Studies at the University of Ottawa, the only research unit outside of Ukraine predominantly devoted to the study of contemporary Ukraine, is announcing a new competition of the Drs. Peter and Doris Kule Doctoral Scholarships on Contemporary Ukraine. The Scholarships will consist of an annual award of $22,000, with all tuition waived, for four years (with the possibility of adding a fifth year).

The Scholarships were made possible by a generous donation of $500,000 by the Kule family, matched by the University of Ottawa. Drs. Peter and Doris Kule, from Edmonton, have endowed several chairs and research centres in Canada, and their exceptional contributions to education, predominantly in Ukrainian Studies, has recently been celebrated in the book Champions of Philanthrophy: Peter and Doris Kule and their Endowments.

Students with a primary interest in contemporary Ukraine applying to, or enrolled in, a doctoral program at the University of Ottawa in political science, sociology and anthropology, or in fields related with the research interests of the Chair of Ukrainian Studies, can apply for a Scholarship. The competition is open to international and Canadian students.

The application for the Kule Scholarship must include a 1000 word research proposal, two letters of recommendation (sent separately by the referees), and a CV and be mailed to Dominique Arel, School of Political Studies, Faculty of Social Sciences Building, Room, 7067, University of Ottawa, 120 University St., Ottawa ON K1N 6N5, Canada. Applications will be considered only after the applicant has completed an application to the relevant doctoral program at the University of Ottawa. Consideration of applications will begin on **1 February 2018** and will continue until the award is announced.

The University of Ottawa is a bilingual university and applicants must have a certain oral and reading command of French. Specific requirements vary across departments.

Students interested in applying for the Scholarships beginning in the academic year 2017-2018 are invited to contact Dominique Arel (darel@uottawa.ca), Chairholder, Chair of Ukrainian Studies, and visit our web site (http://socialsciences.uottawa.ca/ukraine)

#3
Ukrainians Travel Visa-Free

by Gwendolyn Sasse
Carnegie Europe, 26 June 2017
http://ceip.org/2tigk5P

Gwendolyn Sasse is a nonresident senior fellow at Carnegie Europe and director of the Centre for East European and International Studies (ZOiS) in Berlin.

On June 11, 2017, visa-free travel for Ukrainian citizens to EU countries finally became a reality. Ukrainians can now visit any EU member state (with the exception of the UK and Ireland) for up to ninety days within a one-hundred-eighty-day period. They are not allowed to work during these stays, and EU member states enabled themselves to apply a brake should the system be abused, for example by large numbers of asylum seekers or people working illegally.

The long-awaited introduction of visa-free travel has several practical and conceptual impacts. For the moment, the latter are the more important, as few Ukrainians have the required biometric passports and the financial means to travel.

The arrival of the visa-free regime was marked with a party and free concerts in a highly symbolic location: Independence Square in the center of Kyiv. Known in Ukrainian as Maidan, the square's name is linked inextricably to the Euromaidan mass protests of 2013–2014. These demonstrations, directed against the corrupt regime of then Ukrainian president Viktor Yanukovych, were triggered by the president's last-minute decision not to sign a political and economic Association Agreement with the EU.

Several thousand people celebrated in the center of Kyiv on June 11. These celebrations highlighted the first impact of the new visa-free regime: it represents an idea rather than just a legal gateway to hassle-free travel. It symbolizes that Ukraine is European.

The EU had started negotiating visa-free travel with Ukraine over fifteen years ago—the process effectively came to a halt during Yanukovych's presidency. Since his departure, visa-free travel has been the biggest concrete incentive the EU could use in its attempt to stimulate domestic reforms through conditionality. The process was extended several times; the list of legal reforms to be undertaken was long and concrete, from border-control issues to anticorruption; and the monitoring of implementation was rigorous. There is no comparable carrot the EU can offer now short of membership, effectively making it harder to incentivize the reform process from outside.

The ongoing war in Ukraine's eastern Donbas region clearly left a mark on President Petro Poroshenko's speech on June 11. During a meeting with his Slovak counterpart Andrej Kiska at the Ukrainian-Slovak border, Poroshenko equated the introduction of visa-free travel with a final break with Moscow.

Of course, it does not mean this, either from an economic or political perspective or with regard to people-to-people contacts. Many Ukrainians will continue to travel to Russia in the foreseeable future, because Ukrainians have at least as many family connections in Russia as in Western countries, and the costs involved in traveling to Russia are lower.

Moreover, the visa-free regime with the EU requires Ukrainians to acquire an international biometric passport. So far, about 3 million Ukrainians hold such passports. Ukrainian border guards expect a 30 percent increase in passenger traffic.

A survey of about 2,000 residents of Ukraine, conducted by the Ilko Kucheriv Democratic Initiatives Foundation and the Razumkov Center in the week the new regime was introduced, found that one-third of Ukraine's population deemed the introduction of visa-free travel important for them. In particular, residents in western regions closer to the EU border appreciated the visa-free regime.

Only 9 percent of those surveyed said that they already had the required biometric passports. Most of them, a distinctly younger cohort of Ukrainians, were already foreign-passport holders who exchanged one type of passport allowing for international travel for another. By contrast, 66 percent said they had no old or new foreign-travel passport—a slightly higher percentage than in 2013. According to the survey, over 84 percent of the respondents over the age of sixty had no foreign-travel passport, and close to 80 percent of them had no intention of obtaining a passport that gives them the legal right to travel to EU member states.

The new visa regime therefore highlights and potentially increases the generational gap. For the moment, however, there is still widespread ignorance about the details of the regime: only 14 percent of the respondents said they had familiarized themselves with the content of the arrangements.

A tangible impact comes in the form of infrastructure, but even this has a symbolic dimension to it too: the number of direct trains from Kyiv to Polish towns has increased. Ukraine now has a budget airline and is beginning to be included more fully into European flight routes. At one level, these are logistical adjustments; but at another, these changes symbolize the shrinking of physical and political distances and the ultimately porous nature of the EU's outer border.

The ability to travel to the EU without a visa has not gone unnoticed in the occupied territories in the Donbas region. Trips are already being organized from the occupied territories across the front line for people to acquire biometric Ukrainian passports. It is too early to judge how attractive this option will prove in the occupied territories, but for those who choose it, this route reinforces the notion of Ukrainian citizenship.

In the medium term, repeated travel to the EU may have socializing effects, especially on the younger generation of Ukrainians who are already measuring their expectations against the living standards and opportunities in the EU. In turn, the government would feel greater pressure to intensify domestic reforms. Last but not least, a greater number of Ukrainians traveling to the EU would bolster Europeans' familiarity with a country still largely unknown to most EU citizens.

#4
38% of Ukrainians Consider Themselves Europeans – Poll

Ukraine Crisis Media Center, 21 June 2017
http://bit.ly/2sOFwjA

Over a third of Ukrainians emphasize the importance of visa-free regime for the population of the country. On the other hand, only 38% of Ukrainians consider themselves Europeans. It is just 3% more than in 2013. Only 10% of the respondents from the western regions, and 7% from the eastern part of Ukraine are going to get a biometric passport. These poll results were presented by Iryna Bekeshkina, Director of the Ilko Kucheriv Democratic Initiatives Foundation, during a press briefing at the Ukrainian Crisis Media Center. A nationwide survey on the attitude of the population to the visa-free regime was held by the Democratic Initiatives Foundation and the Razumkov Center on June 9-13.

The survey results show significant regional and age differences among the population regarding visa-free travel. "The closer to the West, the higher the percentage of people who consider visa-free regime to be important", – said Ms. Irina. In the west, 11% of the respondents have biometric passports. In the east – only 2.5%. The number of biometric passports is higher among younger respondents. Iryna Bekeshkina emphasized that a significant part of the population does not intend to have any foreign passports at all. The number of people who received a regular passport grew only by 4% compared to 2013. "For me it is an indicator that Ukraine is still far from becoming a European country", – said director of the Democratic Initiatives Foundation.

60% of the respondents said that in order for them to consider themselves Europeans they needed a certain level of material well-being. “There are neither age nor regional differences here”, – Mrs. Iryna said. Hlib Vyshlinskyi, Executive Director of the Centre for Economic Strategy, said that visa-free regime should improve the overall economic situation in the country. “This will facilitate all forms of economic cooperation and encourage new investments in the country,” he stressed.

Aliona Hetmanchuk, Director of the Institute of World Policy, said that according to the poll, 36% of Ukrainians will consider themselves Europeans when the rule of law is established in the country. Serhii Sydorenko, editor-in-chief of the Internet-edition “Europeiska Pravda”, noted that the possibility of suspension of visa-free regime will ensure the further implementation of reforms, in particular judicial and anti-corruption ones. “I do not even imagine theoretically a possibility that Poroshenko, or other government leaders, by their actions in the country could cause cancellation of visa-free regime. This would be a political suicide for them. Therefore, I do not even assume that our leaders will go for such a rollback of reforms, which will activate the reverse of the visa-free regime “, – said Serhii Sydorenko.

A total of 14% got themselves familiar with the rights of entry and stay in the Schengen area. Aliona Hetmanchuk noted that it is necessary to radically change the state communication strategy. “Instead of focusing on what are the requirements of the EU, we need to start talking about what the agreement with the EU gives us,” Mrs. Hetmanchuk underlined.

“It is necessary to screen the readiness of the country on the subject of having the right to be a candidate for EU membership”, – said Aliona Hetmanchuk. She stressed that this would help to establish a constructive dialogue with European countries, one which would not rise negative emotions regarding Ukraine’s entrance into the EU.

#5
Huge Cyber Attack Hits Ukraine, Then Ransomware Goes Global

by Anna Nemtsova
Daily Beast, 27 June 2017
http://thebea.st/2seutl4

Lviv, Ukraine—At about 11:00 on Tuesday morning, local time, Ukraine found itself under a massive cyber attack: dozens of state and private websites and computer systems at strategic companies reported their websites frozen with the same message on the screen that said: “Ooops, your important files encrypted.” Soon, that message was spreading around the world.

The list of companies included the computer systems at Borispol airport, the biggest state power distributor Ukrenergo, several banks and the state mail service.
The systems froze with black and red icons on the screens giving instructions, with one of them suggesting that the users send $300 worth of bitcoins to a certain online address. By midday Ukrainian cyber police reported 22 companies hit by the attack, which the specialists said had a gentle Russian name, a diminutive for Peter: "Petya.A."

One of the Ukrainian companies under attack complained to the cyber specialists that on Tuesday morning all its computers first rebooted, then began to check their memory; and when employees turned their computers off to then plug them back in, they saw the black and red warning, the message from the virus. Ukrainian IT specialists said that the Petya.A virus reminded them of the WannaCry ransomware that recently hit North America, Europe, China, and Japan.

To try to prevent the cyber-plague from spreading, Ukraine's National Police cyber specialists immediately answered calls and checked the affected computers, the department's spokesman, Yaroslav Trakalo, said on his Facebook page. "Cyber police advise to immediately unplug computers working in the network at the first signs of problems," Trakalo said.

By mid-afternoon an advisor to the Interior Minister of Ukraine, Anton Gerashchenko, claimed that the cyber attack was staged by Russian special services as an element of the Kremlin's hybrid war against Kiev: "According to the preliminary information, this is an organized system, a kind of training by the Russian intelligence services," Gerashchenko said. "The attack aims at banks, media, and transport communications," he told Ukraine TV.

Note that all this came at a grim, busy time for Kiev's investigators. Also on Tuesday morning police had to investigate two murder cases. A Mercedes Benz with Colonel Maksim Shapoval, a key intelligence officer, blew up at the corner of Solomenskaya and Alekseyevskaya streets. And then there was the body of a 27-year-old foreign citizen found in his rented Kiev apartment: the foreigner was shot in the head, chest, and arm. Kiev police reports did not state which country the victim came from.

Col. Shapoval was the key person investigating Russia's involvement in the Donbas war in Eastern Ukraine. "The assassinated colonel of the Defense Intelligence of Ukraine was working on proof of Russia's aggression: the victory at the Hague court was achieved, thanks to his work," the Ukrainian Independent Information Agency UNIAN reported on Tuesday, referring. (The U.N. websites with that decision about Russian terrorism in Ukraine are now blank.)

"Shapoval had a good reputation but the case might be even more complicated, as according to some reports he organized security for Voronenkov," a local investigative reporter Yekaterina Sergatskova told The Daily Beast.

Former Russian deputy Voronenkov was gunned down in the heart of Kiev in March. His bodyguard killed the assassin.

If this time police investigation proved that Shapoval was a victim of a bomb planted in his car, which appeared obvious, it would be the second case of the same dark nature in Kiev. Last July somebody planted a bomb and killed a famous journalist and fighter for freedom of speech, Pavel Sheremet, when the reporter was driving to work. Ukraine is still waiting for the results of investigations into that crime.

Meanwhile major Russian companies, including the oil giant Rosneft and Home Credit bank, also complained of a massive hacker attack. Vedomosti newspaper reported WannaCry virus attacking all computers at Rosneft subsidiaries; none of the official Rosneft websites could be opened. Office workers at Modelez, at chocolate producer Alpen Gold and Milka and Mars complained about problems with the same virus Petya. A, attacking computer systems in companies based in Russia.

In Ukraine neither the website of the National Police of Ukraine, nor the official website of the Internal Affairs Ministry could be opened.

"At present SBU specialists jointly with the State Service of Special Communications and Information Protection, and the cyber police department, representatives of anti-virus labs are studying the samples of this piece of ransomware and working on its neutralization," the Ukrainian Security Service, SBU said on its website. " Soon recommendations how to protect yourself from the above-mentioned cyber-attack will be given."

But by the time that message went out, the ransomware was spreading across Europe, and around the world.

#6
How an Entire Nation Became Russia's Test Lab for Cyberwarfare

by Andy Greenberg
Wired, 20 June 2017
http://bit.ly/2ufLyY7

The clocks read zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.

“The hackers don’t want us to finish the movie,” Yasinsky’s wife joked. She was referring to an event that had occurred a year earlier, a cyberattack that had cut electricity to nearly a quarter-million Ukrainians two days before Christmas in 2015. Yasinsky, a chief forensic analyst at a Kiev digital security firm, didn’t laugh. He looked over at a portable clock on his desk: The time was 00:00. Precisely midnight.

Yasinsky’s television was plugged into a surge protector with a battery backup, so only the flicker of images onscreen lit the room now. The power strip started beeping plaintively. Yasinsky got up and switched it off to save its charge, leaving the room suddenly silent.

He went to the kitchen, pulled out a handful of candles and lit them. Then he stepped to the kitchen window. The thin, sandy-blond engineer looked out on a view of the city as he’d never seen it before: The entire skyline around his apartment building was dark. Only the gray glow of distant lights reflected off the clouded sky, outlining blackened hulks of modern condos and Soviet high-rises.

Noting the precise time and the date, almost exactly a year since the December 2015 grid attack, Yasinsky felt sure that this was no normal blackout. He thought of the cold outside—close to zero degrees Fahrenheit—the slowly sinking temperatures in thousands of homes, and the countdown until dead water pumps led to frozen pipes.

That’s when another paranoid thought began to work its way through his mind: For the past 14 months, Yasinsky had found himself at the center of an enveloping crisis. A growing roster of Ukrainian companies and government agencies had come to him to analyze a plague of cyberattacks that were hitting them in rapid, remorseless succession. A single group of hackers seemed to be behind all of it. Now he couldn’t suppress the sense that those same phantoms, whose fingerprints he had traced for more than a year, had reached back, out through the internet’s ether, into his home.

The Cyber-Cassandras said this would happen. For decades they warned that hackers would soon make the leap beyond purely digital mayhem and start to cause real, physical damage to the world. In 2009, when the NSA’s Stuxnet malware silently accelerated a few hundred Iranian nuclear centrifuges until they destroyed themselves, it seemed to offer a preview of this new era. “This has a whiff of August 1945,” Michael Hayden, former director of the NSA and the CIA, said in a speech. “Somebody just used a new weapon, and this weapon will not be put back in the box.”

Now, in Ukraine, the quintessential cyberwar scenario has come to life. Twice. On separate occasions, invisible saboteurs have turned off the electricity to hundreds of thousands of people. Each blackout lasted a matter of hours, only as long as it took for scrambling engineers to manually switch the power on again. But as proofs of concept, the attacks set a new precedent: In Russia’s shadow, the decades-old nightmare of hackers stopping the gears of modern society has become a reality.

And the blackouts weren't just isolated attacks. They were part of a digital blitzkrieg that has pummeled Ukraine for the past three years—a sustained cyberassault unlike any the world has ever seen. A hacker army has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, energy. Wave after wave of intrusions have deleted data, destroyed computers, and in some cases paralyzed organizations' most basic functions. "You can't really find a space in Ukraine where there *hasn't* been an attack," says Kenneth Geers, a NATO ambassador who focuses on cybersecurity.

In a public statement in December, Ukraine's president, Petro Poroshenko, reported that there had been 6,500 cyberattacks on 36 Ukrainian targets in just the previous two months. International cybersecurity analysts have stopped just short of conclusively attributing these attacks to the Kremlin, but Poroshenko didn't hesitate: Ukraine's investigations, he said, point to the "direct or indirect involvement of secret services of Russia, which have unleashed a cyberwar against our country." (The Russian foreign ministry didn't respond to multiple requests for comment.)

To grasp the significance of these assaults—and, for that matter, to digest much of what's going on in today's larger geopolitical disorder—it helps to understand Russia's uniquely abusive relationship with its largest neighbor to the west. Moscow has long regarded Ukraine as both a rightful part of Russia's empire and an important territorial asset—a strategic buffer between Russia and the powers of NATO, a lucrative pipeline route to Europe, and home to one of Russia's few accessible warm-water ports. For all those reasons, Moscow has worked for generations to keep Ukraine in the position of a submissive smaller sibling.

But over the past decade and a half, Moscow's leash on Ukraine has frayed, as popular support in the country has pulled toward NATO and the European Union. In 2004, Ukrainian crowds in orange scarves flooded the streets to protest Moscow's rigging of the country's elections; that year, Russian agents allegedly went so far as to poison the surging pro-Western presidential candidate Viktor Yushchenko. A decade later, the 2014 Ukrainian Revolution finally overthrew the country's Kremlin-backed president, Viktor Yanukovych (a leader whose longtime political adviser, Paul Manafort, would go on to run the US presidential campaign of Donald Trump). Russian troops promptly annexed the Crimean Peninsula in the south and invaded the Russian-speaking eastern region known as Donbass. Ukraine has since then been locked in an undeclared war with Russia, one that has displaced nearly 2 million internal refugees and killed close to 10,000 Ukrainians.

From the beginning, one of this war's major fronts has been digital. Ahead of Ukraine's post-revolution 2014 elections, a pro-Russian group calling itself CyberBerkut—an entity with links to the Kremlin hackers who later breached Democratic targets in America's 2016 presidential election—rigged the website of the country's Central Election Commission to announce ultra-right presidential candidate Dmytro Yarosh as the winner. Administrators detected the tampering less than an hour before the election results were set to be declared. And that attack was just a prelude to Russia's most ambitious experiment in digital war, the barrage of cyberattacks that began to accelerate in the fall of 2015 and hasn't ceased since.

Yushchenko, who ended up serving as Ukraine's president from 2005 to 2010, believes that Russia's tactics, online and off, have one single aim: "to destabilize the situation in Ukraine, to make its government look incompetent and vulnerable." He lumps the blackouts and other cyberattacks together with the Russian disinformation flooding Ukraine's media, the terroristic campaigns in the east of the country, and his own poisoning years ago—all underhanded moves aimed at painting Ukraine as a broken nation. "Russia will never accept Ukraine being a sovereign and independent country," says Yushchenko, whose face still bears traces of the scars caused by dioxin toxicity. "Twenty-five years since the Soviet collapse, Russia is still sick with this imperialistic syndrome."

But many global cybersecurity analysts have a much larger theory about the endgame of Ukraine's hacking epidemic: They believe Russia is using the country as a cyberwar testing ground—a laboratory for perfecting new forms of global online combat. And the digital explosives that Russia has repeatedly set off in Ukraine are ones it has planted at least once before in the civil infrastructure of the United States.

One Sunday morning in October 2015, more than a year before Yasinsky would look out of his kitchen window at a blacked-out skyline, he sat near that same window sipping tea and eating a bowl of cornflakes. His phone rang with a call from work. He was then serving as the director of information security at StarLightMedia, Ukraine's largest TV broadcasting conglomerate. During the night, two of StarLight's servers had inexplicably gone offline. The IT administrator on the phone assured him that the servers had already been restored from backups.

But Yasinsky felt uneasy. The two machines had gone dark at almost the same minute. "One server going down, it happens," Yasinsky says. "But two servers at the same time? That's suspicious."

Resigned to a lost weekend, he left his apartment and took the 40-minute metro ride to StarLightMedia's office. When he got there, Yasinsky and the company's IT admins examined the image they'd kept of one of the corrupted servers. Its master boot record, the deep-seated, reptile-brain portion of a computer's hard drive that tells the machine where to find its own operating system, had been precisely overwritten with zeros. This was especially troubling, given that the two victim servers were domain controllers, computers with powerful privileges that could be used to reach into hundreds of other machines on the corporate network.

Yasinsky quickly discovered the attack was indeed far worse than it had seemed: The two corrupted servers had planted malware on the laptops of 13 StarLight employees. The infection had triggered the same boot-record overwrite technique to brick the machines just as staffers were working to prepare a morning TV news bulletin ahead of the country's local elections.

Nonetheless, Yasinsky could see he'd been lucky. Looking at StarLight's network logs, it appeared the domain controllers had committed suicide prematurely. They'd actually been set to infect and destroy 200 more PCs at the company. Soon Yasinsky heard from a competing media firm called TRK that it had been less fortunate: That company lost more than a hundred computers to an identical attack.

Yasinsky managed to pull a copy of the destructive program from StarLight's network. Back at home, he pored over its code. He was struck by the layers of cunning obfuscation—the malware had evaded all antivirus scans and even impersonated an antivirus scanner itself, Microsoft's Windows Defender. After his family had gone to sleep, Yasinsky printed the code and laid the papers across his kitchen table and floor, crossing out lines of camouflaging characters and highlighting commands to see its true form. Yasinsky had been working in information security for 20 years; he'd managed massive networks and fought off crews of sophisticated hackers before. But he'd never analyzed such a refined digital weapon.

Beneath all the cloaking and misdirection, Yasinsky figured out, was a piece of malware known as KillDisk, a data-destroying parasite that had been circulating among hackers for about a decade. To understand how it got into their system, Yasinsky and two colleagues at StarLight obsessively dug into the company's network logs, combing them again and again on nights and weekends. By tracing signs of the hackers' fingerprints—some compromised corporate YouTube accounts, an administrator's network login that had remained active even when he was out sick—they came to the stomach-turning realization that the intruders had been inside their system for more than six months. Eventually, Yasinsky identified the piece of malware that had served as the hackers' initial foothold: an all-purpose Trojan known as BlackEnergy.

Soon Yasinsky began to hear from colleagues at other companies and in the government that they too had been hacked, and in almost exactly the same way. One attack had hit Ukrzaliznytsia, Ukraine's biggest railway company. Other targets asked Yasinsky to keep their breaches secret. Again and again, the hackers used BlackEnergy for access and reconnaissance, then KillDisk for destruction. Their motives remained an enigma, but their marks were everywhere.

"With every step forward, it became clearer that our *Titanic*had found its iceberg," says Yasinsky. "The deeper we looked, the bigger it was."

Even then, Yasinsky didn't know the real dimensions of the threat. He had no idea, for instance, that by December 2015, BlackEnergy and KillDisk were also lodged inside the computer systems of at least three major Ukrainian power companies, lying in wait.

At first, Robert Lee blamed the squirrels.

It was Christmas Eve 2015—and also, it so happened, the day before Lee was set to be married in his hometown of Cullman, Alabama. A barrel-chested and bearded redhead, Lee had recently left a high-level job at a three-letter US intelligence agency, where he'd focused on the cybersecurity of critical infrastructure. Now he was settling down to launch his own security startup and marry the Dutch girlfriend he'd met while stationed abroad.

As Lee busied himself with wedding preparations, he saw news headlines claiming that hackers had just taken down a power grid in western Ukraine. A significant swath of the country had apparently gone dark for six hours. Lee blew off the story—he had other things on his mind, and he'd heard spurious claims of hacked grids plenty of times before. The cause was usually a rodent or a bird—the notion that squirrels represented a greater threat to the power grid than hackers had become a running joke in the industry.
The next day, however, just before the wedding itself, Lee got a text about the purported cyberattack from Mike Assante, a security researcher at the SANS Institute, an elite cybersecurity training center. That got Lee's attention: When it comes to digital threats to power grids, Assante is one of the most respected experts in the world. And he was telling Lee that the Ukraine blackout hack looked like the real thing.

Just after Lee had said his vows and kissed his bride, a contact in Ukraine messaged him as well: The blackout hack was real, the man said, and he needed Lee's help. For Lee, who'd spent his career preparing for infrastructure cyberattacks, the moment he'd anticipated for years had finally arrived. So he ditched his own reception and began to text with Assante in a quiet spot, still in his wedding suit.

Lee eventually retreated to his mother's desktop computer in his parents' house nearby. Working in tandem with Assante, who was at a friend's Christmas party in rural Idaho, they pulled up maps of Ukraine and a chart of its power grid. The three power companies' substations that had been hit were in different regions of the country, hundreds of miles from one another and unconnected. "This was not a squirrel," Lee concluded with a dark thrill.

By that night, Lee was busy dissecting the KillDisk malware his Ukrainian contact had sent him from the hacked power companies, much as Yasinsky had done after the StarLightMedia hack months before. ("I have a very patient wife," Lee says.) Within days, he'd received a sample of the BlackEnergy code and forensic data from the attacks. Lee saw how the intrusion had started with a phishing email impersonating a message from the Ukrainian parliament. A malicious Word attachment had silently run a script on the victims' machines, planting the BlackEnergy infection. From that foothold, it appeared, the hackers had spread through the power companies' networks and eventually compromised a VPN the companies had used for remote access to their network—including the highly specialized industrial control software that gives operators remote command over equipment like circuit breakers.

Looking at the attackers' methods, Lee began to form a notion of who he was up against. He was struck by similarities between the blackout hackers' tactics and those of a group that had recently gained some notoriety in the cybersecurity world—a group known as Sandworm. In 2014 the security firm FireEye had issued warnings about a team of hackers that was planting BlackEnergy malware on targets that included Polish energy firms and Ukrainian government agencies; the group seemed to be developing methods to target the specialized computer architectures that are used for remotely managing physical industrial equipment. The group's name came from references to Dune found buried in its code, terms like Harkonnen and Arrakis, an arid planet in the novel where massive sandworms roam the deserts.

No one knew much about the group's intentions. But all signs indicated that the hackers were Russian: FireEye had traced one of Sandworm's distinctive intrusion techniques to a presentation at a Russian hacker conference. And when FireEye's engineers managed to access one of Sandworm's unsecured command-and-control servers, they found instructions for how to use BlackEnergy written in Russian, along with other Russian-language files.

Most disturbing of all for American analysts, Sandworm's targets extended across the Atlantic. Earlier in 2014, the US government reported that hackers had planted BlackEnergy on the networks of American power and water utilities. Working from the government's findings, FireEye had been able to pin those intrusions, too, on Sandworm.

For Lee, the pieces came together: It looked like the same group that had just snuffed out the lights for nearly a quarter-million Ukrainians had not long ago infected the computers of American electric utilities with the very same malware.

It had been just a few days since the Christmas blackout, and Assante thought it was too early to start blaming the attack on any particular hacker group—not to mention a government. But in Lee's mind, alarms went off. The Ukraine attack represented something more than a faraway foreign case study. "An adversary that had already targeted American energy utilities had crossed the line and taken down a power grid," Lee says. "It was an imminent threat to the United States."

On a cold, bright day a few weeks later, a team of Americans arrived in Kiev. They assembled at the Hyatt, a block from the golden-domed Saint Sophia Cathedral. Among them were staff from the FBI, the Department of Energy, the Department of Homeland Security, and the North American Electric Reliability Corporation, the body responsible for the stability of the US grid, all part of a delegation that had been assigned to get to the bottom of the Ukrainian blackout.

The Feds had also flown Assante in from Wyoming. Lee, a hotter head than his friend, had fought with the US agencies over their penchant for secrecy, insisting that the details of the attack needed to be publicized immediately. He hadn't been invited.

On that first day, the suits gathered in a sterile hotel conference room with the staff of Kyivoblenergo, the city's regional power distribution company and one of the three victims of the power grid attacks. Over the next several hours, the Ukrainian company's stoic execs and engineers laid out the blow-by-blow account of a comprehensive, almost torturous raid on their network.

As Lee and Assante had noticed, the malware that infected the energy companies hadn't contained any commands capable of actually controlling the circuit breakers. Yet on the afternoon of December 23, Kyivoblenergo employees had watched helplessly as circuit after circuit was opened in dozens of substations across a Massachusetts-sized region, seemingly commanded by computers on their network that they couldn't see. In fact, Kyivoblenergo's engineers determined that the attackers had set up their own perfectly configured copy of the control software on a PC in a faraway facility and then had used that rogue clone to send the commands that cut the power.

Once the circuit breakers were open and the power for tens of thousands of Ukrainians had gone dead, the hackers launched another phase of the attack. They'd overwritten the firmware of the substations' serial-to-ethernet converters—tiny boxes in the stations' server closets that translated internet protocols to communicate with older equipment. By rewriting the obscure code of those chunks of hardware—a trick that likely took weeks to devise—the hackers had permanently bricked the devices, shutting out the legitimate operators from further digital control of the breakers. Sitting at the conference room table, Assante marveled at the thoroughness of the operation.

The hackers also left one of their usual calling cards, running KillDisk to destroy a handful of the company's PCs. But the most vicious element of the attack struck the control stations' battery backups. When the electricity was cut to the region, the stations themselves also lost power, throwing them into darkness in the midst of their crisis. With utmost precision, the hackers had engineered a blackout within a blackout.
"The message was, 'I'm going to make you feel this everywhere.' *Boom boom boom boom boom boom boom*," Assante says, imagining the attack from the perspective of a bewildered grid operator. "These attackers must have seemed like they were gods."
That night, the team boarded a flight to the western Ukrainian city of Ivano-Frankivsk, at the foot of the Carpathian Mountains, arriving at its tiny Soviet-era airport in a snowstorm. The next morning they visited the headquarters of Prykarpattyaoblenergo, the power company that had taken the brunt of the pre-Christmas attack.

The power company executives politely welcomed the Americans into their modern building, under the looming smokestacks of the abandoned coal power plant in the same complex. Then they invited them into their boardroom, seating them at a long wooden table beneath an oil painting of the aftermath of a medieval battle.

The attack they described was almost identical to the one that hit Kyivoblenergo: BlackEnergy, corrupted firmware, disrupted backup power systems, KillDisk. But in this operation, the attackers had taken another step, bombarding the company's call centers with fake phone calls—possibly to delay any warnings of the power outage from customers or simply to add another layer of chaos and humiliation.

There was another difference too. When the Americans asked whether, as in Kiev, cloned control software had sent the commands that shut off the power, the Prykarpattyaoblenergo engineers said no, that their circuit breakers had been opened by another method. That's when the company's technical director, a tall, serious man with black hair and ice-blue eyes, cut in. Rather than try to explain the hackers' methods to the Americans through a translator, he offered to show them, clicking Play on a video he'd recorded himself on his battered iPhone 5s.

The 56-second clip showed a cursor moving around the screen of one of the computers in the company's control room. The pointer glides to the icon for one of the breakers and clicks a command to open it. The video pans from the computer's Samsung monitor to its mouse, which hasn't budged. Then it shows the cursor moving again, seemingly of its own accord, hovering over a breaker and attempting again to cut its flow of power as the engineers in the room ask one another who's controlling it.

The hackers hadn't sent their blackout commands from automated malware, or even a cloned machine as they'd done at Kyivoblenergo. Instead, the intruders had exploited the company's IT helpdesk tool to take direct control of the mouse movements of the stations' operators. They'd locked the operators out of their own user interface. And before their eyes, phantom hands had clicked through dozens of breakers—each serving power to a different swath of the region—and one by one by one, turned them cold.

In August 2016, eight months after the first Christmas blackout, Yasinsky left his job at StarLightMedia. It wasn't enough, he decided, to defend a single company from an onslaught that was hitting every stratum of Ukrainian society. To keep up with the hackers, he needed a more holistic view of their work, and Ukraine needed a more coherent response to the brazen, prolific organization that Sandworm had become. "The light side remains divided," he says of the balkanized reaction to the hackers among their victims. "The dark side is united."

So Yasinsky took a position as the head of research and forensics for a Kiev firm called Information Systems Security Partners. The company was hardly a big name. But Yasinsky turned it into a de facto first responder for victims of Ukraine's digital siege.

Not long after Yasinsky switched jobs, almost as if on cue, the country came under another, even broader wave of attacks. He ticks off the list of casualties: Ukraine's pension fund, the country's treasury, its seaport authority, its ministries of infrastructure, defense, and finance. The hackers again hit Ukraine's railway company, this time knocking out its online booking system for days, right in the midst of the holiday travel season. As in 2015, most of the attacks culminated with a KillDisk-style detonation on the target's hard drive. In the case of the finance ministry, the logic bomb deleted terabytes of data, just as the ministry was preparing its budget for the next year. All told, the hackers' new winter onslaught matched and exceeded the previous year's—right up to its grand finale.

On December 16, 2016, as Yasinsky and his family sat watching Snowden, a young engineer named Oleg Zaychenko was four hours into his 12-hour night shift at Ukrenergo's transmission station just north of Kiev. He sat in an old Soviet-era control room, its walls covered in beige and red floor-to-ceiling analog control panels. The station's tabby cat, Aza, was out hunting; all that kept Zaychenko company was a television in the corner playing pop music videos.

He was filling out a paper-and-pencil log, documenting another uneventful Saturday evening, when the station's alarm suddenly sounded, a deafening continuous ringing. To his right Zaychenko saw that two of the lights indicating the state of the transmission system's circuits had switched from red to green—in the universal language of electrical engineers, a sign that it was off.

The technician picked up the black desk phone to his left and called an operator at Ukrenergo's headquarters to alert him to the routine mishap. As he did, another light turned green. Then another. Zaychenko's adrenaline began to kick in. As he hurriedly explained the situation to the remote operator, the lights kept flipping: red to green, red to green. Eight, then 10, then 12.

As the crisis escalated, the operator ordered Zaychenko to run outside and check the equipment for physical damage. At that moment, the 20th and final circuit switched off and the lights in the control room went out, along with the computer and TV. Zaychenko was already throwing a coat over his blue and yellow uniform and sprinting for the door. The transmission station is normally a vast, buzzing jungle of electrical equipment stretching over 20 acres, the size of more than a dozen football fields. But as Zaychenko came out of the building into the freezing night air, the atmosphere was eerier than ever before: The three tank-sized transformers arrayed alongside the building, responsible for about a fifth of the capital's electrical capacity, had gone entirely silent. Until then Zaychenko had been mechanically ticking through an emergency mental checklist. As he ran past the paralyzed machines, the thought entered his mind for the first time: The hackers had struck again.

This time the attack had moved up the circulatory system of Ukraine's grid. Instead of taking down the distribution stations that branch off into capillaries of power lines, the saboteurs had hit an artery. That single Kiev transmission station carried 200 megawatts, more total electric load than all the 50-plus distribution stations knocked out in the 2015 attack combined. Luckily, the system was down for just an hour—hardly long enough for pipes to start freezing or locals to start panicking—before Ukrenergo's engineers began manually closing circuits and bringing everything back online.

But the brevity of the outage was virtually the only thing that was less menacing about the 2016 blackout. Cybersecurity firms that have since analyzed the attack say that it was far more evolved than the one in 2015: It was executed by a highly sophisticated, adaptable piece of malware now known as "CrashOverride," a program expressly coded to be an automated, grid-killing weapon.

Lee's critical infrastructure security startup, Dragos, is one of two firms that have pored through the malware's code; Dragos obtained it from a Slovakian security outfit called ESET. The two teams found that, during the attack, CrashOverride was able to "speak" the language of the grid's obscure control system protocols, and thus send commands directly to grid equipment. In contrast to the laborious phantom-mouse and cloned-PC techniques the hackers used in 2015, this new software could be programmed to scan a victim's network to map out targets, then launch at a preset time, opening circuits on cue without even having an internet connection back to the hackers. In other words, it's the first malware found in the wild since Stuxnet that's designed to independently sabotage physical infrastructure.

And CrashOverride isn't just a one-off tool, tailored only to Ukrenergo's grid. It's a reusable and highly adaptable weapon of electric utility disruption, researchers say. Within the malware's modular structure, Ukrenergo's control system protocols could easily be swapped out and replaced with ones used in other parts of Europe or the US instead.

Marina Krotofil, an industrial control systems security researcher for Honeywell who also analyzed the Ukrenergo attack, describes the hackers' methods as simpler and far more efficient than the ones used in the previous year's attack. "In 2015 they were like a group of brutal street fighters," Krotofil says. "In 2016, they were ninjas." But the hackers themselves may be one and the same; Dragos' researchers have identified the architects of CrashOverride as part of Sandworm, based on evidence that Dragos is not yet ready to reveal.

For Lee, these are all troubling signs of Sandworm's progress. I meet him in the bare-bones offices of his Baltimore-based critical infrastructure security firm, Dragos. Outside his office window looms a series of pylons holding up transmission lines. Lee tells me that they carry power 18 miles south, to the heart of Washington, DC.
For the first time in history, Lee points out, a group of hackers has shown that it's willing and able to attack critical infrastructure. They've refined their techniques over multiple, evolving assaults. And they've already planted BlackEnergy malware on the US grid once before. "The people who understand the US power grid know that it can happen here," Lee says.

To Sandworm's hackers, Lee says, the US could present an even more convenient set of targets should they ever decide to strike the grid here. US power firms are more attuned to cybersecurity, but they are also more automated and modern than those in Ukraine—which means they could present more of a digital "attack surface." And American engineers have less experience with manual recovery from frequent blackouts.

No one knows how, or where, Sandworm's next attacks will materialize. A future breach might target not a distribution or transmission station but an actual power plant. Or it could be designed not simply to turn off equipment but to *destroy*it. In 2007 a team of researchers at Idaho National Lab, one that included Mike Assante, demonstrated that it's possible to hack electrical infrastructure to death: The so-called Aurora experiment used nothing but digital commands to permanently wreck a 2.25-megawatt diesel generator. In a video of the experiment, a machine the size of a living room coughs and belches black and white smoke in its death throes. Such a generator is not all that different from the equipment that sends hundreds of megawatts to US consumers; with the right exploit, it's possible that someone could permanently disable power-generation equipment or the massive, difficult-to-replace transformers that serve as the backbone of our transmission system. "Washington, DC? A nation-state could take it out for two months without much issue," Lee says.

In fact, in its analysis of CrashOverride, ESET found that the malware may already include one of the ingredients for that kind of destructive attack. ESET's researchers noted that CrashOverride contains code designed to target a particular Siemens device found in power stations—a piece of equipment that functions as a kill-switch to prevent dangerous surges on electric lines and transformers. If CrashOverride is able to cripple that protective measure, it might already be able to cause permanent damage to grid hardware.

An isolated incident of physical destruction may not even be the worst that hackers can do. The American cybersecurity community often talks about "advanced persistent threats"—sophisticated intruders who don't simply infiltrate a system for the sake of one attack but stay there, silently keeping their hold on a target. In his nightmares, Lee says, American infrastructure is hacked with this kind of persistence: transportation networks, pipelines, or power grids taken down again and again by deep-rooted adversaries. "If they did that in multiple places, you could have up to a month of outages across an entire region," he says. "Tell me what *doesn't* change dramatically when key cities across half of the US don't have power for a month."

It's one thing, though, to contemplate what an actor like Russia *could* do to the American grid; it's another to contemplate why it *would*. A grid attack on American utilities would almost certainly result in immediate, serious retaliation by the US. Some cybersecurity analysts argue that Russia's goal is simply to hem in America's own cyberwar strategy: By turning the lights out in Kiev—and by showing that it's capable of penetrating the American grid—Moscow sends a message warning the US not to try a Stuxnet-style attack on Russia or its allies, like Syrian dictator Bashar al-Assad. In that view, it's all a game of deterrence.

But Lee, who was involved in war-game scenarios during his time in intelligence, believes Russia might actually strike American utilities as a retaliatory measure if it ever saw itself as backed into a corner—say, if the US threatened to interfere with Moscow's military interests in Ukraine or Syria. "When you deny a state's ability to project power, it has to lash out," Lee says.

People like Lee have, of course, been war-gaming these nightmares for well over a decade. And for all the sophistication of the Ukraine grid hacks, even they didn't really constitute a catastrophe; the lights did, after all, come back on. American power companies have already learned from Ukraine's victimization, says Marcus Sachs, chief security officer of the North American Electric Reliability Corporation. After the 2015 attack, Sachs says, NERC went on a road show, meeting with power firms to hammer into them that they need to shore up their basic cybersecurity practices and turn off remote access to their critical systems more often. "It would be hard to say we're not vulnerable. Anything connected to something else is vulnerable," Sachs says. "To make the leap and suggest that the grid is milliseconds away from collapse is irresponsible."

But for those who have been paying attention to Sandworm for almost three years, raising an alarm about the potential for an attack on the US grid is no longer crying wolf. For John Hultquist, head of the team of researchers at FireEye that first spotted and named the Sandworm group, the wolves have arrived. "We've seen this actor show a capability to turn out the lights and an interest in US systems," Hultquist says. Three weeks after the 2016 Kiev attack, he wrote a prediction on Twitter and pinned it to his profile for posterity: "I swear, when Sandworm Team finally nails Western critical infrastructure, and folks react like this was a huge surprise, I'm gonna lose it."

The headquarters of Yasinsky's firm, Information Systems Security Partners, occupies a low-lying building in an industrial neighborhood of Kiev, surrounded by muddy sports fields and crumbling gray high-rises—a few of Ukraine's many lingering souvenirs from the Soviet Union. Inside, Yasinsky sits in a darkened room behind a round table that's covered in 6-foot-long network maps showing nodes and connections of Borgesian complexity. Each map represents the timeline of an intrusion by Sandworm. By now, the hacker group has been the consuming focus of his work for nearly two years, going back to that first attack on StarLightMedia.

Yasinsky says he has tried to maintain a dispassionate perspective on the intruders who are ransacking his country. But when the blackout extended to his own home four months ago, it was "like being robbed," he tells me. "It was a kind of violation, a moment when you realize your own private space is just an illusion."

Yasinsky says there's no way to know exactly how many Ukrainian institutions have been hit in the escalating campaign of cyberattacks; any count is liable to be an underestimate. For every publicly known target, there's at least one secret victim that hasn't admitted to being breached—and still other targets that haven't yet discovered the intruders in their systems.

When we meet in ISSP's offices, in fact, the next wave of the digital invasion is already under way. Behind Yasinsky, two younger, bearded staffers are locked into their keyboards and screens, pulling apart malware that the company obtained just the day before from a new round of phishing emails. The attacks, Yasinsky has noticed, have settled into a seasonal cycle: During the first months of the year, the hackers lay their groundwork, silently penetrating targets and spreading their foothold. At the end of the year, they unleash their payload. Yasinsky knows by now that even as he's analyzing last year's power grid attack, the seeds are already being sown for 2017's December surprises.

Bracing for the next round, Yasinsky says, is like “studying for an approaching final exam.” But in the grand scheme, he thinks that what Ukraine has faced for the past three years may have been just a series of practice tests.

He sums up the attackers’ intentions until now in a single Russian word: *poligon.* A training ground. Even in their most damaging attacks, Yasinsky observes, the hackers could have gone further. They could have destroyed not just the Ministry of Finance’s stored data but its backups too. They probably could have knocked out Ukrenergo’s transmission station for longer or caused permanent, physical harm to the grid, he says—a restraint that American analysts like Assante and Lee have also noted. “They’re still playing with us,” Yasinsky says. Each time, the hackers retreated before accomplishing the maximum possible damage, as if reserving their true capabilities for some future operation.

Many global cybersecurity analysts have come to the same conclusion. Where better to train an army of Kremlin hackers in digital combat than in the no-holds-barred atmosphere of a hot war inside the Kremlin’s sphere of influence? “The gloves are off. This is a place where you can do your worst without retaliation or prosecution,” says Geers, the NATO ambassador. “Ukraine is not France or Germany. A lot of Americans can’t find it on a map, so you can practice there.” (At a meeting of diplomats in April, US secretary of state Rex Tillerson went so far as to ask, “Why should US taxpayers be interested in Ukraine?”)

In that shadow of neglect, Russia isn’t only pushing the limits of its technical abilities, says Thomas Rid, a professor in the War Studies department at King’s College London. It’s also feeling out the edges of what the international community will tolerate. The Kremlin meddled in the Ukrainian election and faced no real repercussions; then it tried similar tactics in Germany, France, and the United States. Russian hackers turned off the power in Ukraine with impunity—and, well, the syllogism isn’t hard to complete. “They’re testing out red lines, what they can get away with,” Rid says. “You push and see if you’re pushed back. If not, you try the next step.”

What will that next step look like? In the dim back room at ISSP’s lab in Kiev, Yasinsky admits he doesn’t know. Perhaps another blackout. Or maybe a targeted attack on a water facility. “Use your imagination,” he suggests drily.

Behind him the fading afternoon light glows through the blinds, rendering his face a dark silhouette. “Cyberspace is not a target in itself,” Yasinsky says. “It’s a medium.” And that medium connects, in every direction, to the machinery of civilization itself.

Andy Greenberg (@a_greenberg) wrote about Edward Snowden’s work to protect reporters from hackers in issue 25.03.
This article appears in the July issue

#7

Ukrainian Military Modernization and Minsk Peace Process Implications

Atlantic Council Digital Forensic Research Lab (@DFRLab), 16 June 2016
http://bit.ly/2thPRWg
[Link has videos and hyperlinks]

Recent Ukrainian military exercises highlight not only a more capable force but a possible obstacle to peace

The Ukrainian Armed Forces (UAF) recently released military training and exercise videos displaying tanks, artillery, and missile systems prohibited by the Minsk Agreements. While these exercises are part of the process to modernize Ukraine's military and their efforts to meet NATO standards, these capabilities have been seen along the line of contact, in violation of Minsk peace process.

A training video released on June 11 shows participating battalions using T-64, T-72, and T-80 main battle tanks (MBT). These tanks are armed with 125mm guns, a calibre larger than permitted by the Minsk agreements.

Another video from June 8 displays a likely 9K35 Strela-10 (NATO reporting name: SA-13 "Gopher") surface-to-air-missile (SAM) system, a likely 9K38 "Igla" man-portable SAM (NATO reporting name: SA-18 "Grouse") or variant, and main battle tanks. The Organization for Security and Co-operation in Europe (OSCE) Special Monitoring Mission (SMM) to Ukraine regularly reports Ukrainian heavy weapons violations including the 9K35 Strela-10 and main battle tanks.

On May 26, Ukrainian President Petro Poroshenko was present during a successful "Vilha" 9K58 "Smerch" missile test. The "Vilha" is a 300mm tactical ballistic missile multiple rocket launch system (MLRS) with a 300km range. The Ukrainian Ministry of Defense first reported successful tests of this system in April 2016.

When Russia invaded Crimea and the Donetsk and Luhansk Oblasts in 2014, the Ukrainian military was practically nonexistent and reliant on volunteer battalions to fend off separatist forces and Russian invaders. Western militaries and NATO partners stepped in to support the development and modernization of Ukraine's armed forces into a fully-fledged formal military via bilateral and multilateral platforms.

The Ukrainian Ministries of Defense and Foreign Affairs frequently executepolicies and actions towards the goal to meet NATO military standards in Ukraine's own military, security, and defense operations. In January 2017, Ukrainian President Petro Poroshenko signed a decree approving plans for multinational military training exercises through the NATO Partnership for Peace program, extending U.S.-Ukraine multilateral military exercises such as Sea Breeze and Rapid Trident and international exercises for the next calendar year. Most recently, Ukraine modernized its military medical infrastructure along NATO standards. As the conflict in eastern Ukraine continues to rage on, military modernization and development is expected. However, lack of adherence continues to hinder negotiated peace agreements.

The OSCE SMM includes a section on the withdrawal of heavy weapons in their daily reports. This includes the presence and use of prohibited heavy weapons in areas that should be disarmed in accordance to peace agreements. Lack of adherence to the agreements by both sides leads to civilian casualties, damage to residential areas and infrastructure, and limits the abilities of the OSCE SMM to fulfill their mandate to monitor.

The heavy weapons prohibited by the Minsk Agreements are described as imprecise and indiscriminate as they do not target specific points, but rather hit parts of a larger area. These types of weapons lead to larger numbers of casualties and are as likely to damage surrounding civilian areas than opposing military positions. In the past two weeks, the OSCE SMM observed remarkably high levels of fighting despite the SMM's limited observation abilities after the April 23 security incident [see "First OSCE Monitor Dies in Ukrainian Conflict" –UKL]. These high levels of kinetic activity correlate with high casualty numbers. The UAF reported fifteen killed in action and seventy-six wounded in action from June 1–14, similar numbers to entire months in the past.

Ukraine's goals to meet NATO military standards are leading to a more capable armed forces, as clearly demonstrated in the Ukrainian Anti-Terrorist Operation's (ATO) Press Center social media posts. Consequently, more capable forces are breaking the ceasefire and breaching peace agreements that are essential for positive progress in the east.

#8

Russia, Not Ukraine, Is Serial Violator of Ceasefire Agreement

by John E. Herbst
Atlantic Council, 21 June 2017
http://bit.ly/2tVfv0o

John E. Herbst is the director of the Dinu Patriciu Eurasia Center at the Atlantic Council; he served as US Ambassador to Ukraine from 2003 to 2006.

Like many articles and analyses of the Minsk process, "Ukrainian Military Progress Could Violate Minsk Peace Process" requires additional analysis on the geopolitical underpinnings and implications of the issue at hand. Without this context, it is difficult to make sense of any facts presented.

The context is this: Moscow is conducting the war in Ukraine's east; without Russian leadership, troops, financing, and weapons, there would be no war. Both the EU and the United States levied sanctions to encourage Moscow to end its aggression and to discourage it from the expanding the war further into Ukraine.

Equally important is that fact that the sanctions were levied not long before the Minsk I Agreement was negotiated in September 2014, but Moscow's continuing aggression included the seizure of hundreds of square kilometers of additional Ukrainian territory. A Russian offensive violating Minsk I led to the negotiation of the Minsk II Agreement in February 2015, with terms far more negative for Ukraine. Those terms delayed the return of border control to Ukraine and permitted the Russian-controlled separatists to maintain their own military forces.

The bottom line is clear: Moscow is conducting a low intensity war in the Donbas to destabilize the government in Ukraine by producing regular Ukrainian casualties, seizing small increments of additional Ukrainian territory, and overtaxing the economy.

None of this appears in "Ukrainian Military Progress Could Violate Minsk Peace Process." This is perhaps not surprising as the article is part of a generally superb series produced by DFRLab that is focused on reporting on open source information and social media, which it works to prove or disprove, rather than providing policy analysis.

But even here there is a problem because the article talks only about the possible Minsk violations by one party to the conflict, and the victim at that. This approach ignores the fact that the Russians and their proxies are responsible for most of the violations, and that Ukrainian violations are often in response to Moscow's. The Ukrainians recognize that Russian violations have led to the loss of additional territory with no serious response from the West.

Ukrainian troops are adamant that they don't respond with banned weapons. "If they shoot at us with mortars, we respond with machine guns," Ivan Burdiuh, a press officer for the 30th Brigade, told *The Daily Signal* in February.

The best source of unbiased data about the fighting in the Donbas comes from the OSCE Special Monitoring Mission in Ukraine. Since the OSCE operates on consensus and Russia is a member, the OSCE Special Monitoring Mission (SMM) must be cautious in how it puts out information. While it reports violations on a daily basis, it does not aggregate them. And most of the violations that it reports are described as "undetermined."

Still the SMM daily reports, if aggregated, yield useful information beyond the intensity of the ceasefire violations. In May, for example, the OSCE SMM reported that the Ukrainian side suffered the impact of 945 explosions, while the Russian side experienced only 145. The Russians have likewise proved a greater obstacle to SMM staff's movements. In May, the Russians blocked access to SMM personnel 82 times, while Ukrainians blocked access 54 times. Such data are much more relevant to evaluate the ceasefire than the possible presence of new Ukrainian weapon systems near the line of contact.

Any reporting on the security situation in Ukraine and violations of the Minsk Agreement should be met with a healthy degree of skepticism and often requires deeper policy analysis. Highlighting peripheral developments at the expense of constant ceasefire violations and ignoring context is both misleading and dangerous. It feeds the agenda of those who would like to end sanctions on Moscow. They argue that both Moscow and Kyiv are violating Minsk; therefore, there is no reason for disadvantaging Moscow by maintaining sanctions. It is not in our interests to provide ammunition to those who fail to address who is both the aggressor and the serial violator of Minsk.

#9
Ukrainian Military Intelligence Officer Killed by Car Bomb in Kiev

By Alec Luhn
Guardian, 27 June 2017
http://bit.ly/2sd7ZAA

Col Maksim Shapoval, who was head of a special forces unit, killed and passersby injured in terrorist act, government says

A high-ranking Ukrainian military intelligence official has been killed by a car bomb in Kiev in what authorities are calling an act of terrorism.

An explosive device destroyed the Mercedes being driven by Col Maksim Shapoval at 8.15am local time, police said.

The car's bonnet was blown open and its roof and driver side door almost completely destroyed, video footage from the scene showed.

"The picture of the crime looks like it was a planned act of terrorism," interior ministry spokesman Artem Shevchenko told local media. The military prosecutor said his office would lead an investigation.

Police said a female passerby with shrapnel wounds to her legs received medical treatment after the explosion, as did an elderly man who suffered shrapnel wounds to his neck.

According to the defence ministry, Shapoval was a colonel in military intelligence. The Ukrainian Pravda newspaper quoted law enforcement sources saying he had headed a special forces unit.

Yury Butusov, editor of the Censor.net news website, said in a Facebook post that Shapoval's unit had fought in eastern Ukraine, where a conflict with Russia-backed separatists that broke out in 2014 has killed more than 10,000 people. He claimed Russian intelligence could have killed Shapoval.

Shapoval's death comes almost a year after prominent journalist Pavel Sheremet was killed by a similar explosion in Kiev as he drove to work. A documentary film released last month revealed evidence suggesting that Ukraine's spy agency may have witnessed the planting of the car bomb that killed Sheremet. No one has been brought to justice in the murder case.

A number of other public figures have also been assassinated in and around Kiev in recent years. Denis Voronenkov, a former Russian MP who fled to Ukraine, was shot dead in central Kiev in March. Pro-Russian journalist Oles Buzina was shot in a drive-by in 2015, and lawyer Yuri Grabovsky, who had represented a Russian soldier captured in Ukraine, was found dead with a gunshot wound in 2016.

#10
Ukraine's Military Reveals Details about Russian Members of Sabotage Group

By Will Ponomarenko
Kyiv Post, 27 June 2017
http://bit.ly/2tlNW3d

Ukraine's military has revealed more details about a sabotage group, which included three Russian citizens, that it says it eliminated in Luhansk Oblast on June 24.

"Last week, Ukraine received yet more evidence of Russian involvement in the fighting in eastern Ukraine," Defense Ministry spokesman Vilyen Pidgorny said during a briefing in Kyiv on June 26.

Ukraine's armed forces reported on June 24 that it had intercepted a group of six enemy soldiers near the P-66 road, which runs west from the occupied city of Luhansk and forms part of the front line in the area.

According to Pidgorny, two of the fighters were medics, both Russians, and four others were identified as infantrymen, one of whom was Russian national.

Ukraine's military press service, reporting the incident on June 25, said that two of the enemy soldiers were killed during a firefight with Ukrainian forces. One of those killed was the squad's commander, a Russian national originally from the city of Kirov, the press service said. Two other Russian soldiers, the medics, were captured.

“One Russian citizen (of two captured medics) is a resident of the Altai Krai (region), which is located more than 3,000 kilometers from eastern Ukraine,” Pidgorny said. He did not give any details about the other captured Russian soldier.

The military press service said the group was armed with two Kalashnikov machine guns, two SVD sniper rifles, two AK-74 assault rifles, and an RPG-26 grenade launcher. “Documents that indicate that detainees served within the ranks of Russian occupation forces and proof of their Russian origin has been transferred to state security officers of Ukraine for further examination,” Pidgorny said.

Later, on the evening of June 26, the press service of the 93rd Mechanized Brigade, the military unit responsible for defending the area along the P-66 road, published a statement on the incident on the unit’s Facebook page.

The statement, quoting the brigade’s commander, Colonel Vladyslav Klochkov, identified the killed squad commander as regular from the Russian army, Captain Alexander Scherbak, going by the codename “Alex”, who also served as a commando instructor.

Under the Russian captain’s command, the enemy group attempted to attack Ukrainian forces near the village of Zhelobok, according to Klochkov.

“Having gained a tactical advantage over the enemy, our servicemen suggested that they surrender, with guarantees for their lives and safety,” the brigade’s statement reads. “The squad commander and a sniper made an attempt to put up armed resistance and were killed in close combat.”

The brigade said that the captured Russian soldier from the Altai Krai Region was 22 years old.

The brigade’s Facebook post also shows images of the enemy soldiers’ weapons captured after the clash. In particular, the brigade said the SVD sniper rifles were made in 1994, and of a type designed and produced exclusively for the Russian army.

The 93rd brigade also said in its Facebook message that it had captured other modern Russian equipment designed for Russian military sabotage groups, but it gave no details.

#11

Disconnected Society: How the War in the Donbas Has Affected Ukraine

by Kateryna Iakovlenko
OpenDemocracy, 26 June 2017
http://bit.ly/2sjPO7u

People displaced by the war in eastern Ukraine need a community to represent their interests - any community. Why is that proving so difficult?

Kateryna Iakovlenko is a journalist and researcher from Rovenky, Luhansk. She researches Ukrainian art of the 1980s-1990s, and is postgraduate student at the New Media Department, Lviv National University.

An Italian journalist once asked me why I love my country. He also asked me whether I consider myself Ukrainian. After all, I was born in the Donbas, and I speak mostly Russian in my everyday life. But just because my home is now a war zone and my mother tongue is Russian doesn't make me any less a citizen of Ukraine, or infringe my ability to relate to my country with respect, love and healthy criticism.

Recently, I was asked another question at a Kyiv hospital. I'd gone to register at the clinic, and the clerk behind the desk asked where I was registered previously. When I replied "Luhansk region", she answered: "Oh, you're not a separatist by any chance?" This kind of question would stop anybody in their tracks. And perhaps we could joke about it, if that phrase didn't conceal a war and the lives of people who are dear to me.

The strength of stereotypes

The stigmatisation of people from the Donbas often happens precisely on the everyday level, with everyday people, in everyday life. People take the example set by politicians, who have never said publicly: "We are all residents of one country and we are all needed here, every person who has a Ukrainian passport is worth the attention and care of our state, whichever part of the world they might be in."

Before the war, the issues of language and where you're registered as living didn't seem particularly important. Many things can be taken as given when there isn't a war going on: you cross the street when the light turns green; cars drive on the right side of the road; when someone steals your pursue, you go to the police station; and if you live in a country, you take care to improve it and make it more comfortable, just as that country takes care of you, too.

A state relies on functioning communities - professional associations, groups that gather around certain interests and so on. Debates within these groups and between them allow the whole of society to remain healthy and capable of evaluating situations critically, find solutions and defend its interests. In turn, the comfort of these groups and their active public position guarantees an equal society, one with the power and confidence in its own rights and obligations.

Totemic solidarity

Before the war, society in Donetsk was made up into small local communities. Some people liked theatre, some were artists, others were activists (both on the left and the right), there was an intelligentsia oriented around the sciences and the arts, and so on. There were also ongoing divisions inside these communities. But as violent events began to develop in the region from 2013 onwards, these communities split up even more, disintegrating into even smaller units.

But there's solidarity in this story, too. And it's worth mentioning it, so that these communities can start working again to find possible ways of defending their interests.

On 21 November 2013, when students, programmers and journalists came out onto the Maidan in Kyiv, five people paid a visit to the monument to Taras Shevchenko, Ukraine's national poet, in Donetsk. These people were representatives of different communities, but inside their groups they turned out to be the only people who decided to demonstrate publicly in support of EuroMaidan. One of the first people to do so was Evgeny Nasadyuk, a director and playwright, who works under the name Pyotr Armyanovsky. This demonstration, which initially attracted five people, grew gradually, with 10 people, then 50. Over the course of several months, active residents of Donetsk stayed close to the Shevchenko monument for days on end.

By January 2014, this kind of demonstration became impossible. The activists in Donetsk began to be attacked more regularly, there was more violence on the streets, and the violence was starting to slip of out of control.

Teenagers armed with bats would attack the demonstrators, and they remained unpunished despite the fact that the city police was still functioning, and the plan to reorganise it hadn't arisen. One way of scaring the activists was to douse them with zelyonka, the green dye used to humiliate politicians and other persons of interest.

A few months passed and people who called themselves residents of Donetsk came out to protest allegedly against the values of EuroMaidan. In the twisted logic of this protest, the problem of defending the region's Russophone population and their human rights (which was also linked to language) somehow emerged. In the media, this demonstration received the name "Anti-Maidan", as something opposed to the protests happening in Kyiv.

All five activists who came out to protest in Donetsk in November 2013 spoke Russian. They were all residents of the Donbas, and now they are all displaced people. They demonstrated to assert their rights as citizens of Ukraine, to protest against corruption in society and all institutions of power, to support modernisation and the improvement of the country's education system. These values are universal, and thus there's no room for exclusion on regional or other grounds here.

The largest demonstration, called "pro-Ukrainian" by activists and the press, took place in April 2014. Here, it was the same "five and fifty activists" who'd stood in front of the monument to Shevchenko previously. Indeed, it was the image of this demonstration, which showed a Ukrainian flag flying on Lenin Square in Donetsk, that went viral.

But it wouldn't be quite accurate to call this protest "pro-Ukrainian". For the people on Lenin Square, the most important motivating factor wasn't the Ukrainian national idea (although that was also present), but resisting the spontaneous violence that had begun to spread not only through the city's streets, but its institutions too, thus alienating the city's residents. It was precisely opposition to violence that became an important element for people trying to assert humanist ideals and democratic principles in April 2014. All of this helped reinvigorate Donetsk's local community for a time, its importance and faith in the idea that city residents could defend their city.

Although this protest was mostly attended by Russian speakers, the Ukrainian flag became its main symbol. This choice was not an accidental one. The Ukrainian flag expressed hope of retaining the state as a force that could defend the city and country against an external threat (many people were worried that the Crimean scenario could be repeated in eastern Ukraine). With the local elite and authorities inactive, the flag became something more than two pieces of blue and yellow material sewn together. It became a totem, a symbol that could protect society from violence. The flag could also be seen as a cry for help - from Kyiv or the international community.

But what happened to this society and its sub-units after violence finally won out here?

The "other" from the Donbas

Three years on, Ukrainian society has changed a lot. Now, nobody remembers the story of the five people who protested in Donetsk in November 2013. The protesters who attended the April 2014 demonstration became internally displaced people, and they moved to different cities. For many, this move became a source of stress, and the problems that arise in new cities (accommodation, work, finances and so on) led to a feeling of being stuck in a hole. Meanwhile, for others, new circumstances gave way to positive changes and even career opportunities (many young people left to study at European universities or took jobs in good companies).

The subject of internally displaced people is one of the most divisive in the western and Ukrainian press. At the beginning of the conflict, displaced people encountered constant discrimination. In conditions of war, the power of stereotypes has only grown stronger. Despite the fact that many articles on tolerance appeared in the Ukrainian press, people displaced from the Donbas were still represented negatively in mass consciousness - poor, uneducated, politically naive and so on. On a personal level, I have encountered similar claims: "You're an exception. But there are others, the majority. After all, it was your region that chose [Viktor] Yanukovych, and now we're going through all of this."

Moreover, those people who stayed in Donetsk have on occasion experienced hostility from residents of other regions of the country: “If you didn’t leave, you must’ve earned it”. At the height of events in spring 2014, I rang a woman who worked at the Donetsk Metallurgical Factory - I’d made a small documentary film with her in the past. She asked me: “What are they saying about us in Kiev? What are they saying in general?” Of course, different things were being said. Maidan fostered the creation of many volunteer organisations (VostokSOS, DonbasSOS, New Mariupol, to name a few) that worked directly with people, helped them with food or money, and even repaired homes for them. Yet another section of society couldn’t understand the situation beyond the stereotypes: apparently, the people who remained in the occupied territories in eastern Ukraine don’t leave precisely because they support the regime there.

The historian Elena Styazhkina has said many times that you shouldn’t call people living in the occupied territories separatists or supporters of the so-called People’s Republics. Indeed, according to Styazhkina, these people should be viewed as hostages - that way, your perception of the situation in the Donbas changes.

Back in 2013, before the war, Sergei Bratkov, a Ukrainian artist from Kharkiv, created the work Leave, Forget, which at the time bore no relation to the conflict. Visually, the work is very simple: a black and white photograph shows a man going down a metro escalator from behind, and on top of it, there’s a neon sign: “leaveforget”. Bratkov’s work was created as a reaction to the relationship between the individual and society, their desire to leave their hometown and move into a different social context. Today, this installation looks completely different: if originally, the man decided to leave due to the soft power of the big city, then today, he’s a resident of the occupied territories who has been physically expelled from his native environment.

Leave and forget - this is all that a certain segment of Ukrainian society wanted people in the Donbas to do in 2014. But in certain situations, it’s impossible to leave, let alone forget. I’ve been asked many times why my parents don’t just leave their region, and whether their reluctance to do so means that life there suits them. I rephrased Bratkov’s sentiment for myself: “Remain and survive”.

Styazhkina notes: “People in the Donbas call themselves peaceful. This isn’t a recognition that the future will be peaceful, but a denial of war. They don’t call themselves republicans or members of the Donetsk People’s Republic. This something of a step towards [peace], and it should be noted. People can move towards this image of the future.”

The emergence of a negative image of the Donbas is connected to the fact that no one outside the region knew much about it, its character, its life, or the people who lived there. People only remember the fact that the Donbas was the heart of Soviet industrialisation, and that people from across the Soviet Union (including some with a criminal past) traveled there to build and restore it after the Second World War. The myth about the down-at-heel Donbas was fed further by gang wars in the early 1990s, as well as the background of its political elite - the majority of them (for example, Rinat Akhmetov or Viktor Yanukovych) had criminal backgrounds. The fact that the region remained conservative and nostalgic for the Soviet past didn't help either.

T he development of this myth, and the opposition between the Donbas and the rest of Ukraine, was useful for political elites who leveraged their influence to gain votes and mobilise the electorate in 1996-2012. Given that real reforms were not being carried out, populist methods were supposed to reorient voters into an emotional frame in which language and birthplace became markers of how Ukrainian society had fallen behind, a barrier to reform, and all responsibility of politicians was removed in favour of an amorphous "regional problem".

The "Sovietness" that the Donbas is often accused of is really the massive gap between the very rich and very poor, the lack of reforms to the education system, the absence of real trade unions, investment in healthcare, low wages, bad transport system and infrastructure, and inactive communities. Indeed, all of these problems unite Ukraine's 24 regions and Crimea.

Realising that the problem of Ukrainian society today isn't its eastern regions, but the substitution of reform with populism, will make everyone feel like a resident of the Donbas - a powerless minority that cannot defend itself. The fear of understanding that Ukrainian society isn't defended by the state leads to the creation of a mythical Other. And this time, Ukraine's Other doesn't come from outer space, but the all-too real Donbas, the source of all the country's ills.

Everyone's a comrade

In spring 2014, before the "Anti-Terrorist Operation" was declared in the Donbas, there was an attempt to create a Committee of Patriotic Forces of Donbas in Donetsk. This was supposed to be a civic initiative that could defend the interests of residents of Donetsk and Luhansk regions at all levels. Despite the fact that the Committee, which includes Donetsk intellectuals and civic activists, still exists today, issues concerning the region are decided mostly without its involvement.

Against the background of the conflict, displaced people could have formed a model of a working community capable of defending its own interests (and the interests of Donetsk and Luhansk) independently. But for the most part, this hasn't happened. And the already fragile community has split up into small groups, which have begun to defend their own interests inside this (small) community, isolating one another and increasing the level of internal competition. This fight, this competition is often accompanied by discussion about which activist is the biggest patriot, who is the biggest activist, who has suffered most, and who has suffered least, and who supports human rights.

For example, when I spoke with Evgeny Nasadyuk in January 2017, he made an offhand remark to the effect that he doesn't want to associate himself with certain representatives of the Donetsk region, and that you should be sceptical about any public demonstrations they organise. Other activists and displaced persons have expressed similar opinions. I experience similar feelings to a certain extent myself. Perhaps this position comes from an unhealed trauma, or the fact that everyone is involved in a secret struggle for their place under the sun. People who refuse to participate in this struggle leave the community and either remain on their own or join another group.

In The Uses of Disorder, the American sociologist Richard Sennett speaks about how “images of communal solidarity are forged in order that men can avoid dealing with each other… The ‘we’ feeling, which expresses the desire to be similar, is a way for men to avoid the necessity of looking deeper into each other.” Ukrainian society isn’t so far from this model: the concept of “us” isn’t formed on the basis of accepting different categories and groups of the population, and even excludes them.

Our segmented society has stopped talking to one another, defining common aims, seeing allies, rather than enemies, in each other. Any discussion is reduced to “kitchen talk”, Facebook activism or posts on other social networks. Street protest doesn’t work anymore, it’s been compromised too many times by paid actions. Furthermore, the people behind Ukraine’s public polemics often come from the same small circle who have the same views and similar backgrounds. To go beyond this circle, you have to get out of your comfort zone, express solidarity with people you haven’t met before, and see problems in their true complexity, beyond personal interest. All of this seems utopian and fraught with problems.

Right now, the war justifies everything - aims, means, fictional solidarity, the lack of protection by the state and excessive public patriotism. All of this only plays into the hands of those political forces which will try to retain their place at the next round of elections and once again appeal to the electorate, and not society.

It’s impossible to even imagine that someone from Ukraine’s political leadership will make a special announcement on television (as president Poroshenko did with Ukraine’s visa-free regime), in which he’d announce that we should make our society more human, or, for instance, make a public example of tolerant behaviour towards residents of our country’s two easternmost regions. Or perhaps lobbyists, intellectuals, writers and philosophers from the Donbas could address Ukraine’s parliament.

Still, I’d like to believe that when the guns stop firing, we will be ready to accept peace and everyone without exception. After all, we’ll have to do it anyway.

#12
Ukraine LGBT Community Marches through Kyiv for Gay Pride Parade

by Darko Janjevic

Deutsche Welle, 18 June 2017
http://bit.ly/2rSPsEZ

Some 2,500 people have taken part in the "March of Equality" in downtown Kyiv, with the authorities deploying thousands of security forces to ensure safety. A group of ultranationalists attempted to disrupt the event.

The participants walked through the center of Ukraine's capital, Kyiv, on Sunday, chanting slogans such as "We're different, we're equal!" and "Ukraine for all!"
"Finally in our country, we are able to come out for our rights and show that we exist," said one participant, Tetyana. "I feel nervous and happy that I can come out and not fear anything."

British Ambassador Judith Gough attended the event, which she said was held in a "fine party atmosphere."

Authorities cordoned off most of the area and deployed around 5,000 police officers to safeguard the parade, which has often been targeted by extremist groups in the past. Although no violence was reported at the Sunday event, the marchers were forced to change their route slightly as a group of around 100 ultranationalists attempted to block one of the streets.

Officials said they detained six protesters who tried to break through the police line. "I'm convinced that this is wrong. It's a sin and it can destroy our country morally," said Irina, a student, who protested the event.

Threatened 'bloodbath'

The day before the manifestation, ultranationalist group Right Sector had warned that their supporters would ensure the parade ended in a "bloodbath."

In 2014, Ukraine authorities canceled the LGBT march after police refused to ensure its safety. A year later, the gay pride event was organized outside of the city center, but lasted only several minutes before conservative protesters disrupted the event and clashed with the participants.

The first successful parade was held in 2016, with police out in force to protect about 1,500 participants.

#13
Ukraine’s Security Service Plans Laws to Criminalize “Propaganda” and Fight pro-Russian Fifth Column

by Halya Coynash
Human Rights in Ukraine, 23 June 2017
http://bit.ly/2tVzCvw

Ukraine’s Security Service [SBU] has set up a special page on Facebook where citizens can effectively denounce their fellow Ukrainians for lack of patriotism. This is all supposed to be part of civic involvement in drawing up amendments to legislation to ensure liability for those involvement in “hybrid warfare serving the Russian aggressor”. Media specialists and rights activists believe that Ukrainian legislation already provides such mechanisms, and that the SBU would be better carrying out its own work on protecting national security, rather than putting forward plans to impose unnecessary restrictions on freedom of speech.

The Head of the SBU, Vasyl Hrytsak, has come out with two statements over the last week or so. The first, on June 15, was a call to “all patriots to share responsibility for the future of Ukraine” and to fight the ‘fifth column’ which Russia began cultivating, he stresses, long before its open attack on Ukraine.

After assurances of the Security Service’s commitment to democratic values and true patriotism, Hrytsak goes on to speak of the alleged need to draw up legislation on criminal liability and the SBU’s willingness to take part in this. He says that their aim is “to provide a legal assessment in the Criminal Code of all forms and methods of hybrid warfare. <> In conditions of aggression, it is not only military statutes that are written in blood, but also laws for traitors and accomplices to the aggressor. That is the force of law”.

The force of law is in its precision and clarity, making it easy to foresee what actions make a person a traitor or accomplice. So far, there is none.

The media widely reported Hrytsak as proposing criminal liability for propaganda. Once again, what does this mean? When does the manipulative use of material and / or downright lies to create a negative view of the government, Ukraine’s ‘anti-terrorist operation’ (or war effort) in Donbas, or of the country’s right to exist become a criminal offence?

Hrytsak also calls for a covenant of “information unity drawn up with Ukrainian journalists for countering the enemy”. He calls Russian propaganda a weapon which Russia uses to try to destroy our faith in freedom of speech and democracy. The response, he says, should be “a boycott of all representatives of the fifth column of the Russian

Federation in the Ukrainian information realm. They should become persona non-grata, with this, he explains, being "the force of public opinion".

This sounds rather better, though the question also arises of what one does about those unwilling to make such a pact, or to observe it. Would they face ostracism or criminal liability?

A second statement on June 20 was somewhat mellower in its tone. Hrytsak is initiating "the creation of a public platform for joint transparent discussion on countering Russian information aggression". He invites specialists, lawyers, journalists and civic activists to take part in "dialogue and cooperation on safeguarding Ukraine's national security".

This would, however, still result in the same: legislation on all forms and methods of hybrid warfare, and criminal liability for those individuals and legal entities "who knowingly take part in it, serving the interests of the Russian aggressor".

"Each patriot of Ukraine can leave their proposals regarding the list of actions posing a threat to Ukraine's national interests and demanding legal response on the Facebook page here or send them to platformazminsbu@gmail.com.

After processing these proposals, Hrytsak says, and taking into account both SBU experience and "leading law practice of EU countries and the USA on countering hybrid warfare", the SBU will initiate public discussion on the proposed amendments to legislation.

Olha Chervakova, Deputy Chair of the parliamentary committee on freedom of speech, told Radio Svoboda that she believes a draft law with amendments to legislation on information security is needed, as are any efforts on countering Russian aggression. She has no problem with the involvement in this of the SBU, since it is they who can provide information about people who pose an immediate danger. She does, however, think that a working group must be drawn up.

Dmytro Zolotukhin, Deputy Minister of Information Policy, says that most prosecutions for public calls on the social network VKontakte to overthrow the constitutional order have resulted in suspended sentences. He notes that law enforcement bodies have "a certain deficit of norms which can be applied, however for a democratic country that is absolutely normal. It is abnormal that we are building a democratic state in conditions of effective war".

Tetyana Popova, a media lawyer, believes that the first statement from the SBU "startled international journalist organizations" and that the second has made a move towards meeting civic concerns. Whether that is at declaration, or comes to something, remains to be seen.   She does not believe that anybody, including the SBU, should interfere with freedom of speech.

The Director of the Institute for Mass Information is even more blunt. Oksana Romanyuk sees no need for such a move since there are sufficient laws in the information sphere.

"I think that the SBU should spend a bit more time on its own tasks and not encroach upon regulation of the flow of information". She believes that the situation in Ukraine both with legislation, and with self-regulating bodies is OK as it is. Her position was shared by Mykhailo Chaplyha from the Office of the Human Rights Ombudsperson.

Although the first question must relate to how genuine the calls for public debate are, this is an emotive subject on which views are very strongly divided, as was seen over the recent blocking of Russian-based social media. The SBU's recent history in this field and especially its most prominent prosecution, that of Ruslan Kotsaba, have not inspired confidence. While Kotsaba's views and his willingness to spread a highly distorted picture on Russian media are repugnant to most of us, the SBU's continuing attempt to call this treason aroused concern in Ukraine and prompted Amnesty International to declare Kotsaba a prisoner of conscience.

Perhaps the above-mentioned deficit of norms is partly to blame for obviously flawed prosecutions like that of Kotsaba. For the moment, statements full of emotive rhetoric and short on specifics and legal clarity do not necessarily inspire confidence.

#14
New Book

Ukrainian Migration to the European Union
Lessons for Migrations Studies
Olena Fedyuk and Marta Kindler, editors
Springer Open, IMISCOE Research Series
December 2016
Free Download: http://bit.ly/2sYikhg

This edit volume provides researchers, policy makers and policy scholars, as well as students, with a comprehensive overview of the migration of Ukrainian nationals to the EU. The research on this topic has been steadily growing in the last decades in a variety of disciplines but so far has not been brought together or thoroughly connected. The chapters in this volume map out existing research and contextualize and historicize migration from Ukraine against a string of crises experienced by Ukraine and the region in the last three decades, from the dissolution of the USSR to changes in the EU borders to the failed economic reforms in independent Ukraine.

The book engages in an impressive overview of major publications available in a variety of disciplines and in several languages, among others Russian, Ukrainian and English. It presents readers with a critical analysis of these authoritative sources linking historic and contemporary texts in order to establish longitudinal perspective on and continuity of the migratory trends and practices. Coverage brings together spatial, temporal, and geopolitical perspectives, offering expert analysis in such areas as economics, immigration policies, history, gender, and migration studies.

The contributions to this book aim to engage in a critical dialogue with existing knowledge; although each chapter in our volume confirms the proliferation of research about Ukrainian migration in a number of disciplines, this research has been highly unsystematic, patchy and often politicized. There is a vast discrepancy in methodologies, data sets that are not comparable and an absence of longitudinal approach. This volume seeks to map out existing research in a variety of disciplines, analyzing its proliferation in certain areas and entering into a constructive debate with the literature as to the development of the research trajectories, the politics of knowledge production and need for further studies.

Table of Contents

#15
New Book

Bahatovymirna suchasnist’
Sotsial’ne vkliuchennia v otsintsi suspil’noho rozvitku
Yuriy Savelyev
Kyïv: VPTs “Kyïvs’kyï universitet”, 2017
Free download: https://goo.gl/DwQY24

The book aims at assessment of level of development and prospects of modernization in European societies within perspective of the capability approach (Sen, 1999), social quality model (Beck, 2001; van der Maesen, Walker, 2005) and emancipative values model of modernization (Inglehart, Welzel, 2005, 2010). It is suggested that more accurate assessment can be achieved via comparative analysis of sociocultural dimensions of modernization one of which is social inclusion.

The first chapter provides thorough examination of sociological discourse of modern society and modernization. Five leading segments of the discourse are identified and a manifold perspective on existing theories of modernity is elaborated. The novelty of the proposed analysis, which is rooted in J.C.Alexander's and W.Zapf's studies, is a focus on profound similitude of different theories of modernity and possibility of simultaneous application of distinct explanatory platforms. Such an application significantly differs from existing traditional vision of sociological discourse of modernity and modernization as subsequent change of theoretical approaches or dramatic competition of alternative research programs. Suggested analysis allows identifying various dimensions of modernity that overall constitute a whole picture of modern society.
The chapter also reveals the limitations and contradictions of current theoretical interpretations of development of society, social evolution, modernization and social change. Differences in understanding of essence of development and evolution in contemporary science and sociology are demonstrated.

Longer abstract: http://bit.ly/2seDnyY

#16
CFUS Scholarly Publications Support Program

The Canadian Foundation for Ukrainian Studies is pleased to announce the CFUS Scholarly Publications Support Program for 2017. The terms of reference are online at http://bit.ly/2rZnQi4.We are kindly asking you to post and share this information with your scholars/authors who may qualify and benefit from this support. Should you or they have any questions, please do not hesitate to contact me.

Best regards,
Natalka Zyla
Executive Administrator

CFUS
620 Spadina Avenue
Toronto, ON M5S 2H4
Canada

416.766.9630
admin@cfus.ca

Purpose
To provide financial assistance for the publication of scholarly works in the field of Ukrainian studies by Canadian academic presses.

Amount

The program provides support annually, up to a maximum of $6,500 or half the cost of publication, whichever is less. Approved grants are issued directly to the publisher and not to the author/originator of the work.

Types of publications supported

The Program supports primarily original works in the field of Ukrainian studies to be published by Canadian academic presses.

Preference is given to works that have secured co-funding arrangements.

What MAY be considered: support for the publication of translations, new postsecondary textbooks, or reprints of works of exceptional scholarly value and need

What will NOT be considered:

- periodicals
- belletristic works
- works already in print at the time of application

Evaluation criteria

Works will be evaluated for their:

- scholarly excellence
- originality by way of advancing the field of knowledge
- usefulness and relevance to scholars and students in the field

Priority will be given to:

- works in English or French
- works of potential use and interest to a broader rather than limited readership
- works dealing with the history, culture, society and heritage of Ukraine and Ukrainians generally

Who may apply

- Any scholar whose original work in the field of Ukrainian studies is to be published by a Canadian academic press
- Preference is given to scholars affiliated with Canadian postsecondary institutions.

Application requirements

Applications must be submitted by the author/originator of the work in question and include the following:

(a) a cover letter from the author/originator of the work in question

(b) a letter from the intended publisher that:

- confirms its intent to publish the book and provides an anticipated date of publication

- confirms that the manuscript has been reviewed independently by recognized authorities in the field and has been recommended by them for publication
- includes complete copies of these reviews; actual names of reviewers may be withheld if they were promised anonymity
- includes author's response to each of the expert/peer reviews

(c) an estimate of the total cost of publication, including a budget breakdown
(d) a statement detailing the financial contribution to be made by the publisher and other funding agencies (if any) towards the total cost of publication
(e) a letter or letters from funding agencies (if these are known) stating dollar commitment to the project
(f) anticipated specifications (number of pages, press run) of the finished work and its anticipated date of publication
(g) a copy of the manuscript's "preliminary material" -- the preface, introduction and table of contents)

The application must include each of the above items (a) through (g); otherwise, the application will be considered incomplete.

The entire submission must be submitted electronically (in PDF format) to admin@cfus.ca to the attention of the CFUS Scholarly Publications Program.
The application deadline is OCTOBER 1. Late submissions will not be considered.

For further information, please email admin@cfus.ca or telephone 416-766-9630.

Credits

A book that receives the foundation's financial support must carry acknowledgment of that support (including the foundation's logo) in a customary manner and place in the book.The publisher shall provide CFUS with three (3) complimentary copies of the publication.

Decision

Decisions regarding applications under this program rest with the foundation's Executive Committee and are final once made.

All submissions (including supporting documentation) are destroyed three months after the announcement of the final decision. No materials are returned to applicants or kept by the foundation.

The foundation reserves the right not to award any grant in years when no submission is deemed worthy of support by the foundation's review committee.

#17
Academic Studies Press welcomes new Acquisitions Editor in Slavic, East European and Central Asian Studies

23 June 2017

ASP welcomes Oleh Kotsyuba as Acquisitions Editor in Slavic, East European and Central Asian Studies

Most recently Dr. Kotsyuba was a College Fellow in Slavic Languages and Literatures at Harvard University. He works on twentieth century and contemporary Russian, Ukrainian, and East European literatures and cultures.

Dr. Kotsyuba's research focuses on literature that struggles to come to terms with the experience of living in authoritarian contexts. His dissertation offered a radical revision of the strategies that culture employs to evade the demands that oppressive regimes impose on art and artists. His study of the works of Ukrainian and Russian writers of the Soviet period broke new ground in reconstructing the conditions of cultural and political transformations in the late Soviet Union.

Dr. Kotsyuba's current project studies the cultural afterlife of oppressive regimes after their formal demise.

He has taught courses that introduce students to Slavic literatures and cultures, allow them to read prolific writers in the original and in translation, discuss and write subtly about complexities of the social and cultural life in Russia, the Soviet Union, Poland, and Ukraine in the nineteenth–twenty-first centuries, while also paying attention to relevant interdisciplinary approaches, social and historical aspects of culture.

UKL 485, 27 June 2017

Dominique Arel, Chair of Ukrainian Studies
University of Ottawa, 559 King Edward Ave., Ottawa ON   K1N 6N5 CANADA
tel 613 562 5800 ext. 3692
fax 613 562 5351