What the Hack?!

Russian Cyber and Information Warfare in Ukraine

Michael Doronio, Henrik Haude, Lukas Werner

Roadmap

1. **An introduction to the region**
   - Why Russia? Why Ukraine?
   - Russia and Ukraine: a common history
   - Russia's strategy in its "Near Abroad"
   - The ongoing conflict in Ukraine

2. **A survey of Russian cyber and information warfare in Ukraine**
   - Intersection of cyber and information warfare
   - Examples of cyber attacks in Ukraine
   - Examples of Russia's information campaign
   - The role of non-state actors and hacktivists
   - Evolution from Georgia to Ukraine

3. **Russian Cyber and Information Warfare Strategy**
   - Why hasn't there been a full-scale cyber war in Ukraine?
   - Information warfare as superior to cyber warfare
   - Effectiveness of Russia information warfare in Ukraine
   - Gerasimov Doctrine

4. Conclusion and discussion

Part 1:

Addressing the Bear in the Room:

Why a Case Study of Russian Cyber Interference in Ukraine?

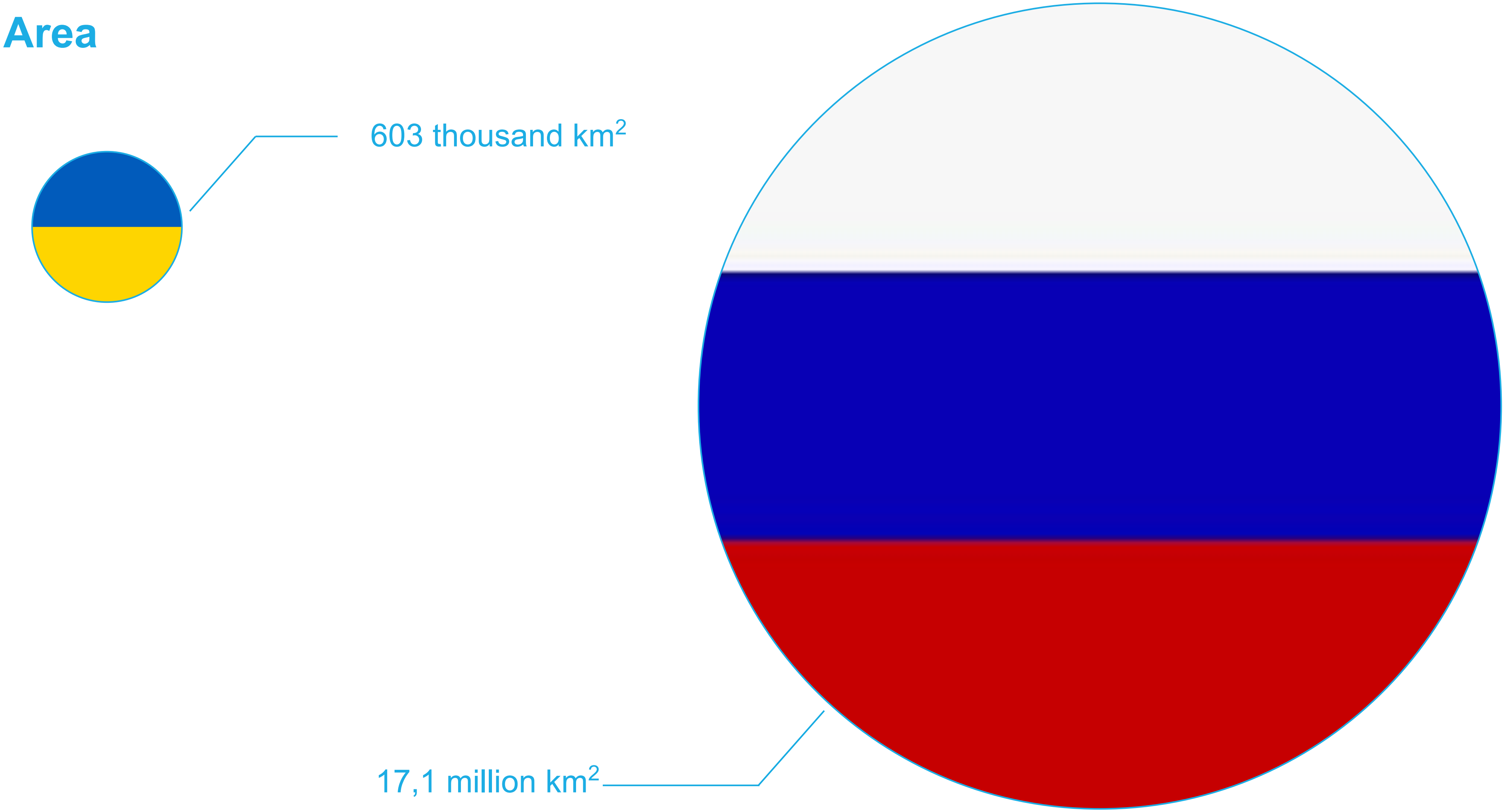
&

Background Information about the Conflict in Ukraine

Why a Case Study of Russia? – Addressing the Bear in the Room

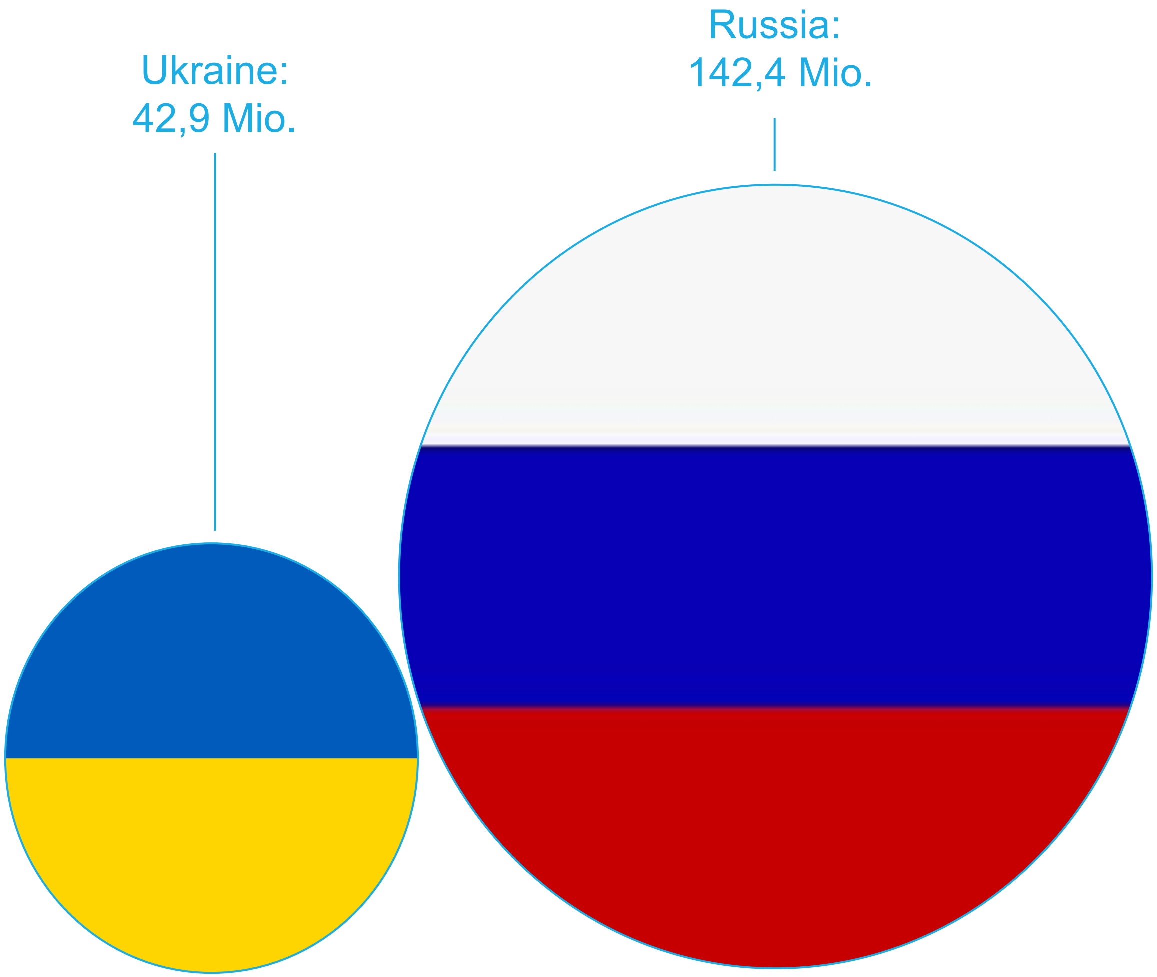
Ukraine: just a small country on the Russian border?

Area



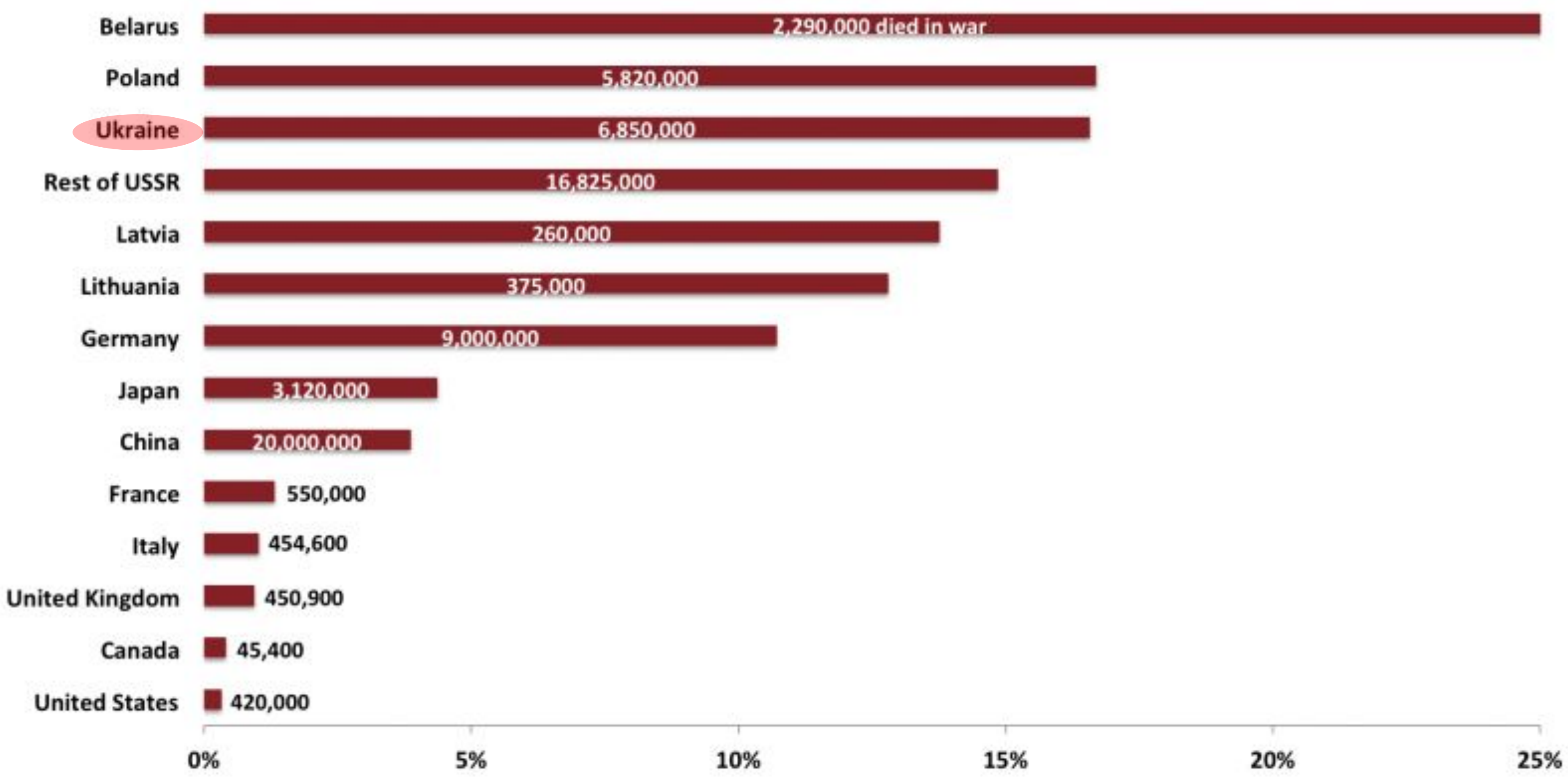
Ukraine matters!

Population

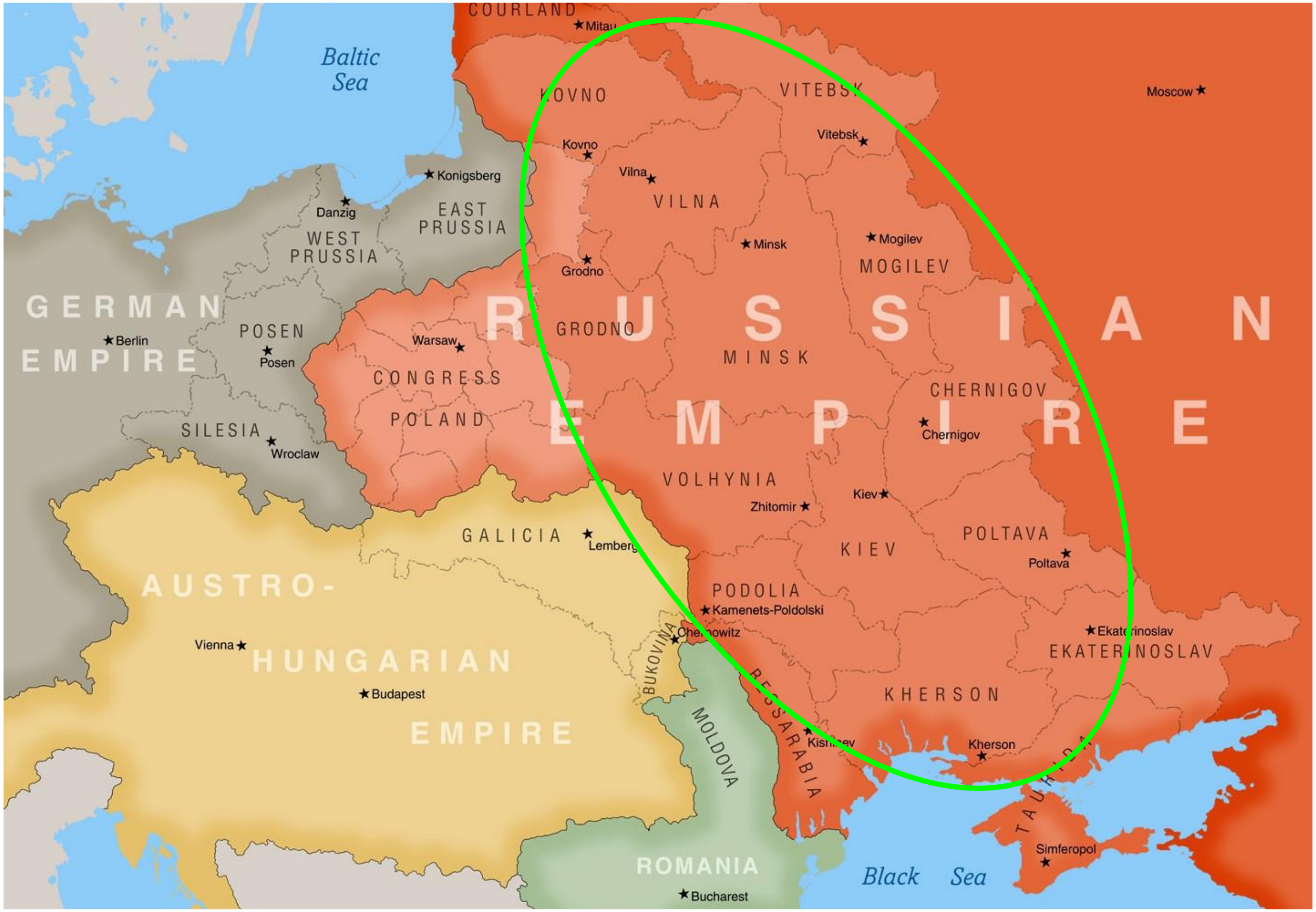


Bloodlands: Ukraine, gateway to Russia

Percentage of the population killed during World War II

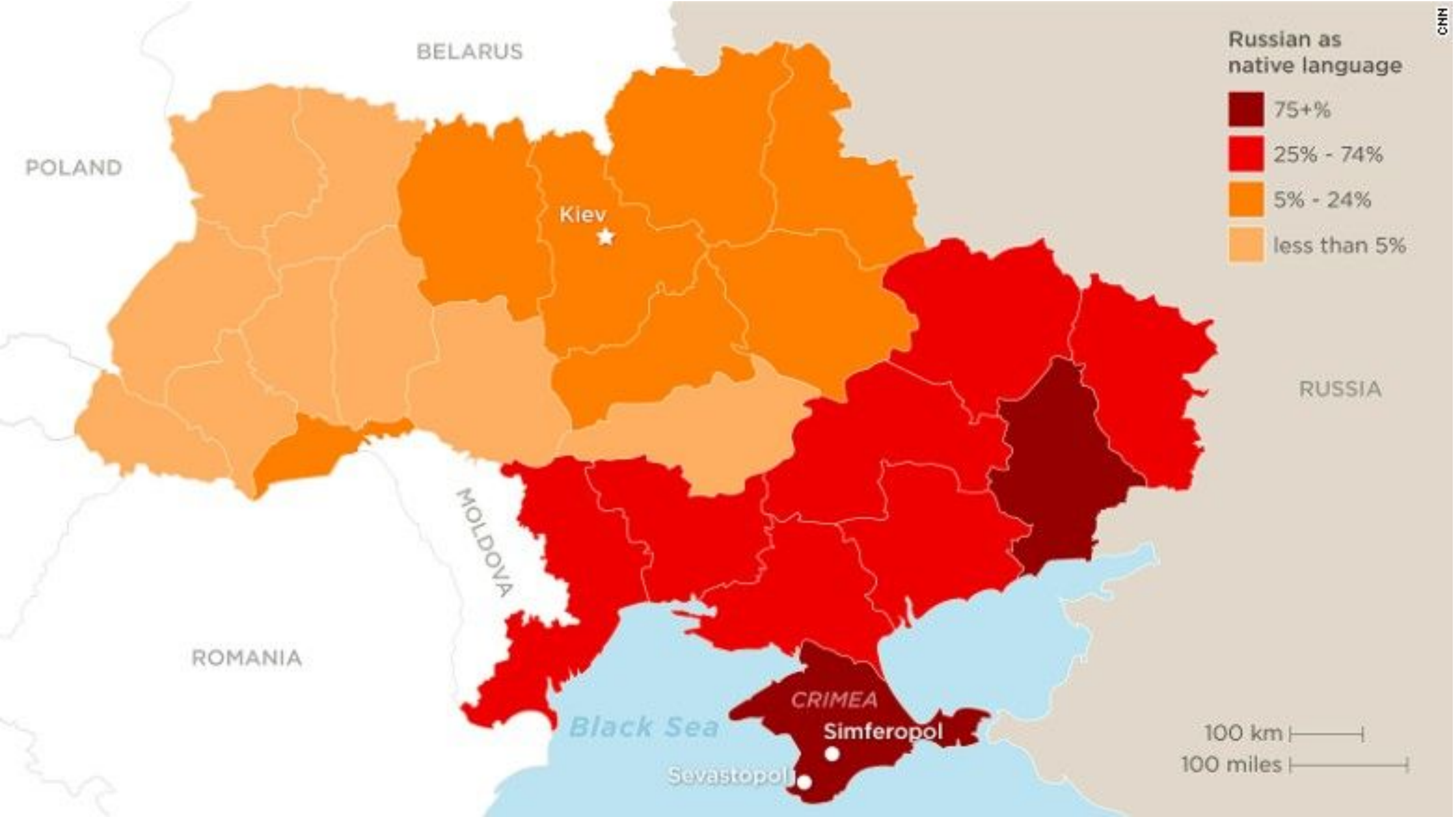


Common History between Russia and Ukraine



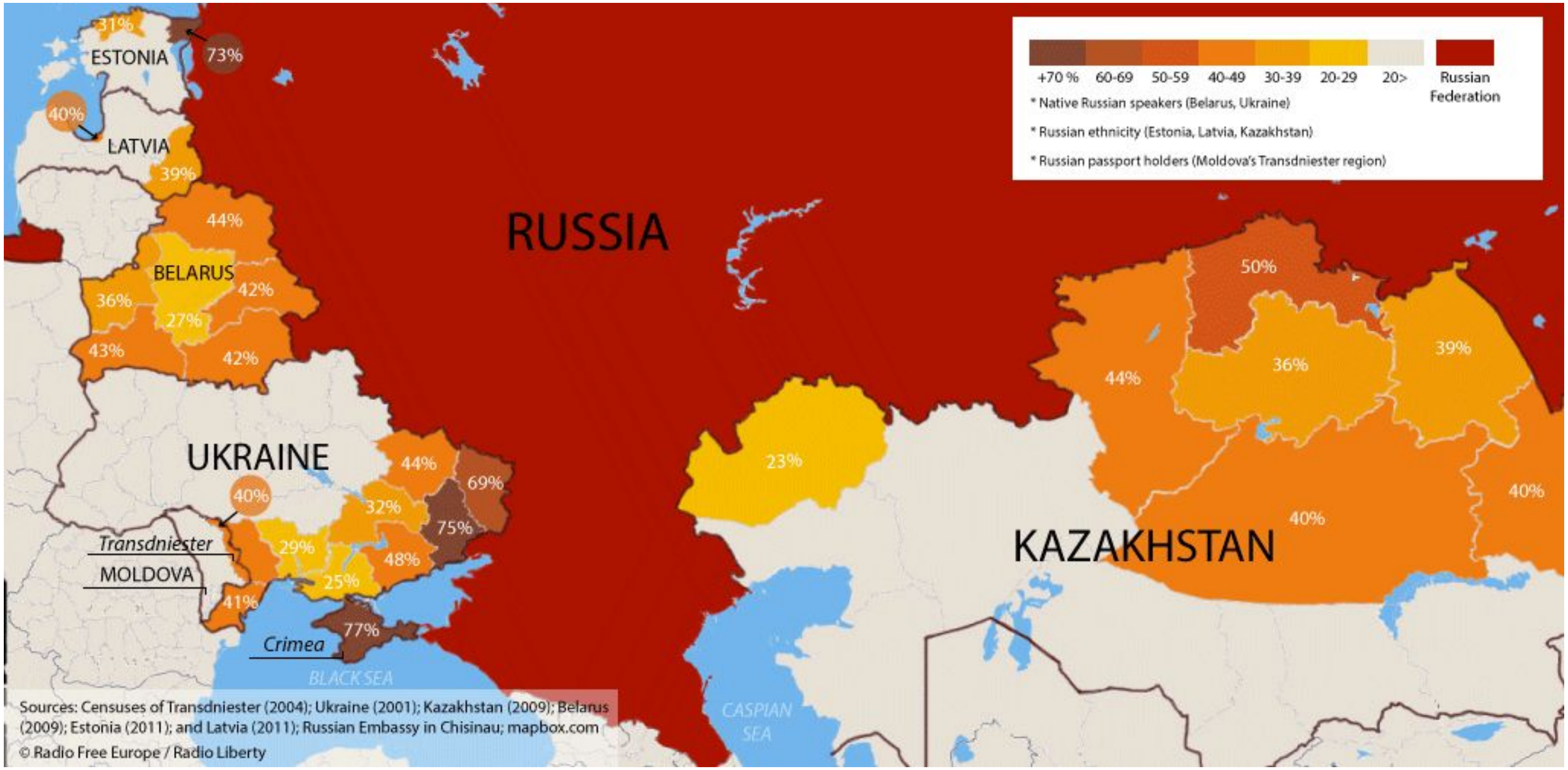
Ukraine as part of the Soviet Union

Russian language plays a huge role in Ukraine



Russia’s “Near abroad”: ethnic Russians and Russian speakers

Regions in Russia’s “Near Abroad” with the greatest concentration of Russian citizens, ethnic Russians and native Russian speakers

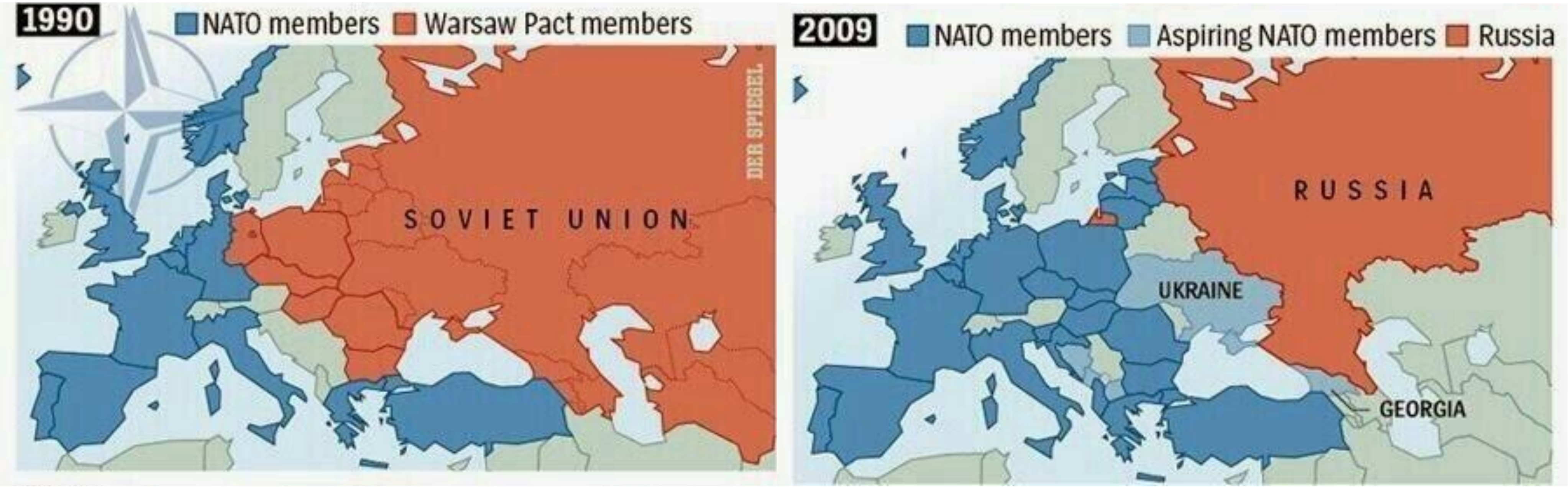


Sources: Censuses of Transdniester (2004); Ukraine (2001); Kazakhstan (2009); Belarus (2009); Estonia (2011); and Latvia (2011); Russian Embassy in Chisinau; mapbox.com
© Radio Free Europe / Radio Liberty

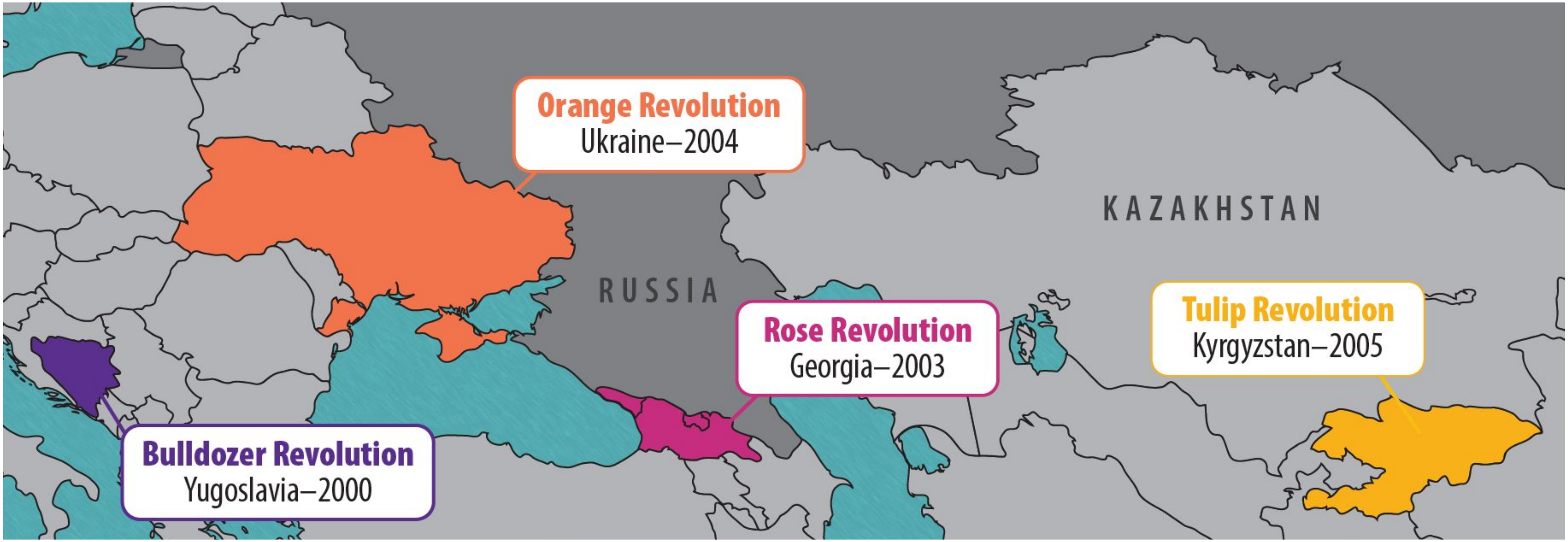
The Kremlin says Moscow will strive to protect the interests of Russian speakers wherever they may be

Security Threat: Russia’s fear of being encircled by NATO

NATO eastward expansion after the fall of the Soviet Union

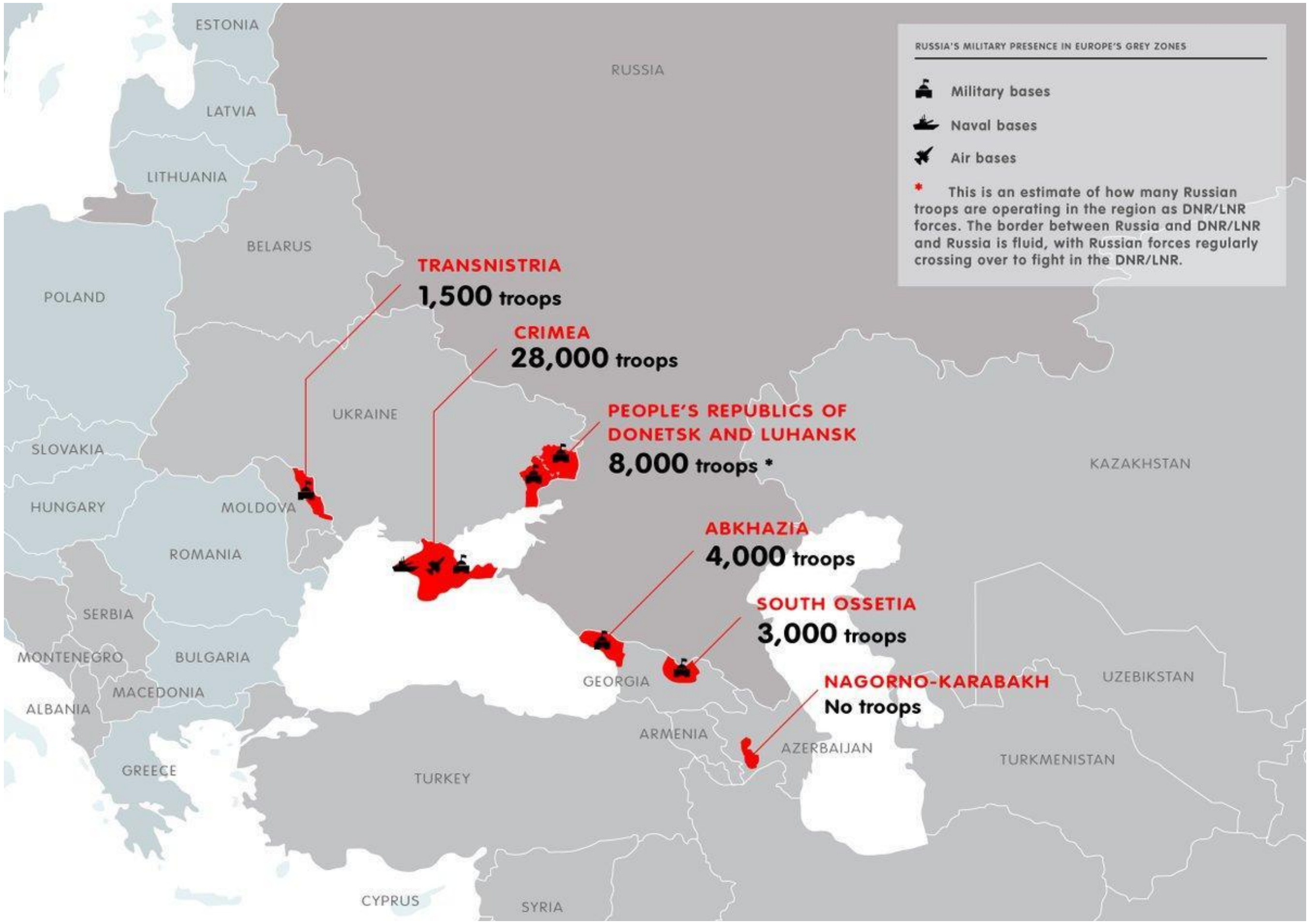


Security Threat: Color Revolutions



"In the modern world extremism is being used as a geopolitical instrument and for remaking spheres of influence. We see what tragic consequences the wave of so-called color revolutions led to -- for us this is a lesson and a warning. We should do everything necessary so that nothing similar ever happens in Russia." **– Vladimir Putin, 2014**

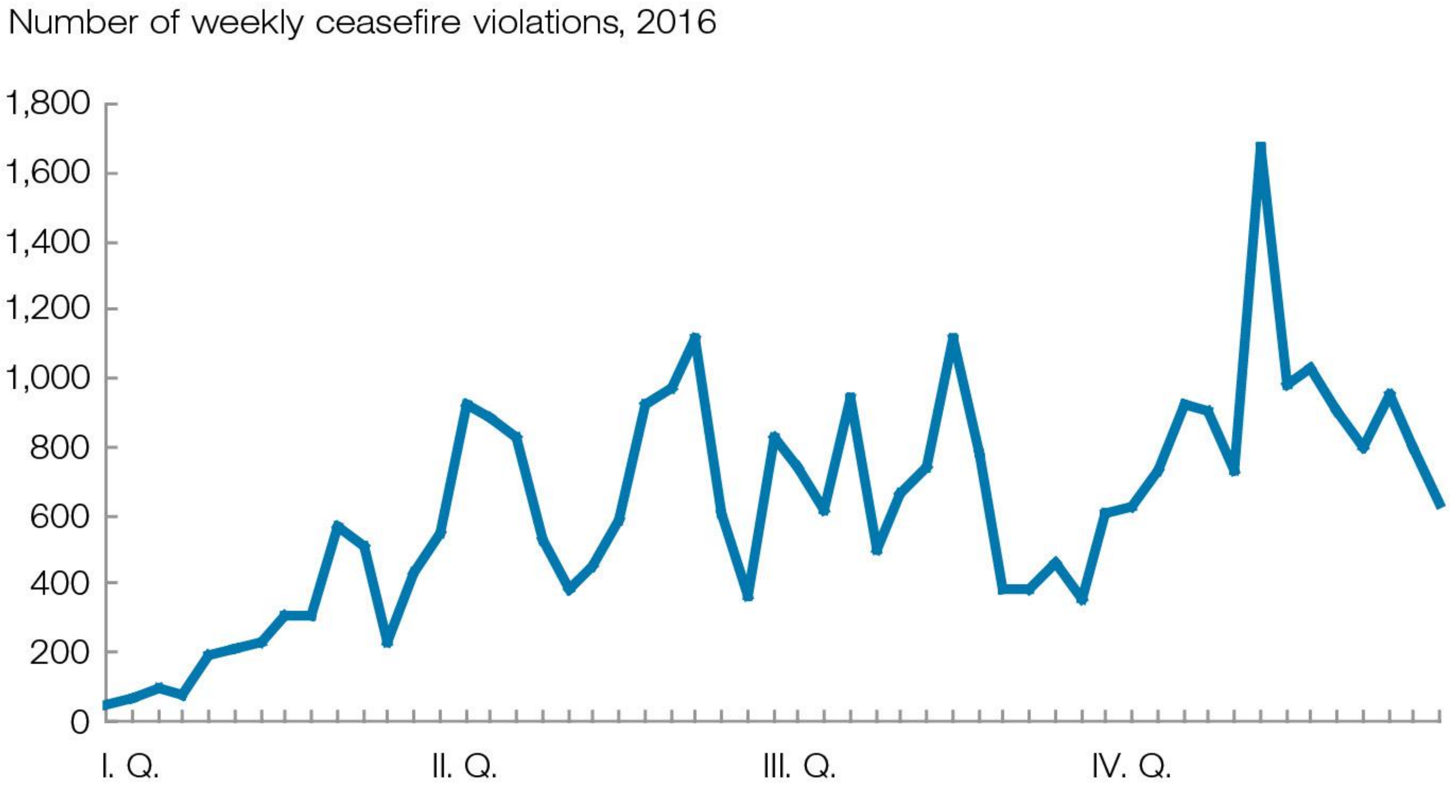
Frozen Conflicts?



Source: IISS Military Balance 2016

A Very Hot Conflict: hostilities continue

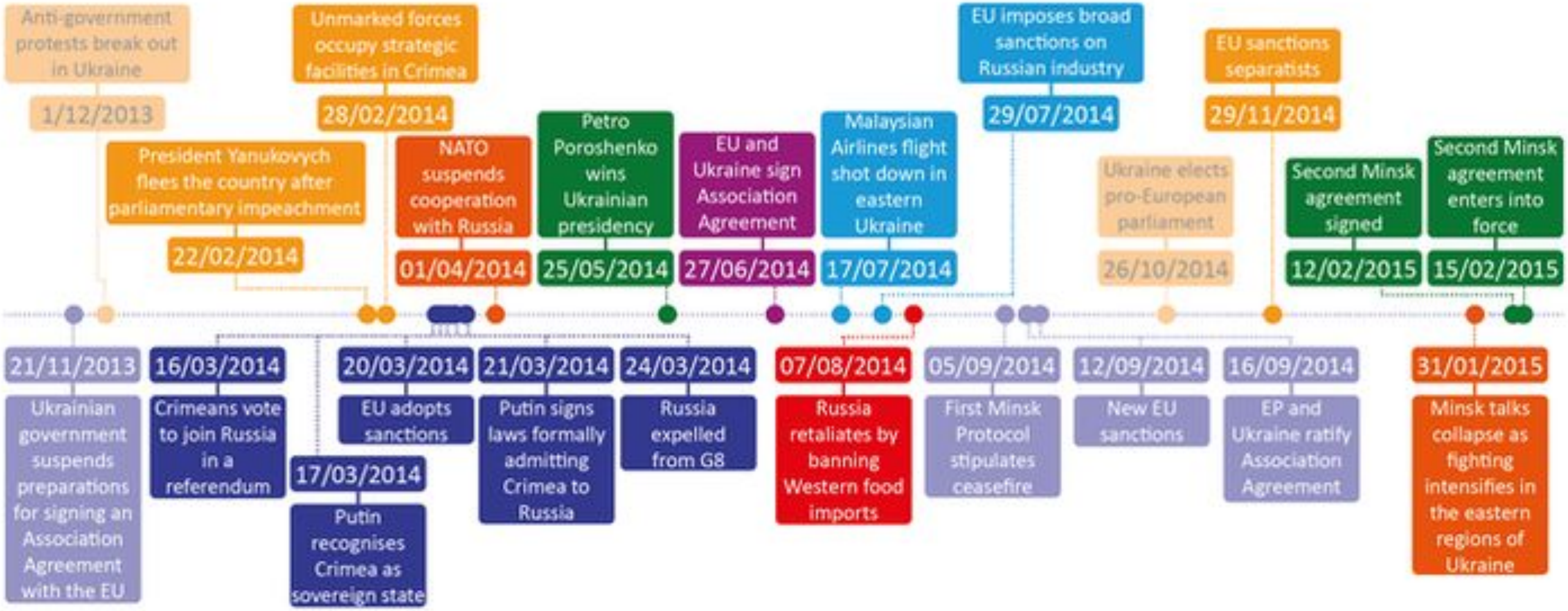
„The conflict in the east is far from frozen, it's the opposite. [...] We can only see a fraction of what is happening, we see the tip of a large, dangerous iceberg.“ **– Alexander Hug (Leiter OSCE SMM)**



Source: Munich Security Report 2017, based on OSCE and Ukraine-Analysen

Timeline of the Conflict in Ukraine

November 2013 – February 2015



21/11/2013 Ukrainian government suspends preparations for signing an Association Agreement with the EU

1/12/2013 Anti-government protests break out in Ukraine

22/02/2014 President Yanukovych flees the country after parliamentary impeachment

28/02/2014 Unmarked forces occupy strategic facilities in Crimea

16/03/2014 Crimeans vote to join Russia in a referendum

17/03/2014 Putin recognises Crimea as sovereign state

20/03/2014 EU adopts sanctions

21/03/2014 Putin signs laws formally admitting Crimea to Russia

24/03/2014 Russia expelled from G8

01/04/2014 NATO suspends cooperation with Russia

25/05/2014 Petro Poroshenko wins Ukrainian presidency

27/06/2014 EU and Ukraine sign Association Agreement

17/07/2014 Malaysian Airlines flight shot down in eastern Ukraine

29/07/2014 EU imposes broad sanctions on Russian industry

07/08/2014 Russia retaliates by banning Western food imports

05/09/2014 First Minsk Protocol stipulates ceasefire

12/09/2014 New EU sanctions

16/09/2014 EP and Ukraine ratify Association Agreement

26/10/2014 Ukraine elects pro-European parliament

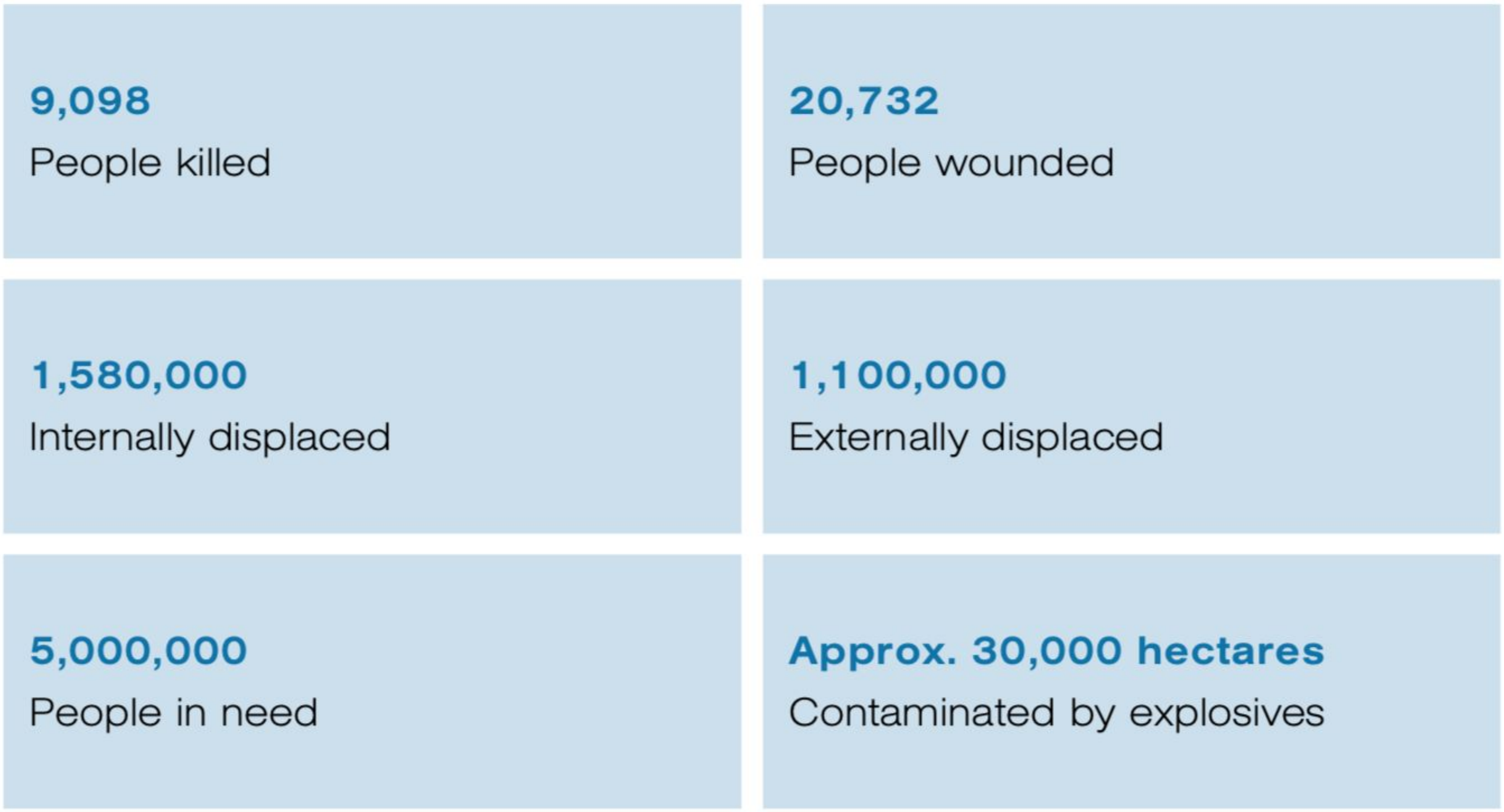
29/11/2014 EU sanctions separatists

31/01/2015 Minsk talks collapse as fighting intensifies in the eastern regions of Ukraine

12/02/2015 Second Minsk agreement signed

15/02/2015 Second Minsk agreement enters into force

Toll of the War in Ukraine



9,098
People killed

20,732
People wounded

1,580,000
Internally displaced

1,100,000
Externally displaced

5,000,000
People in need

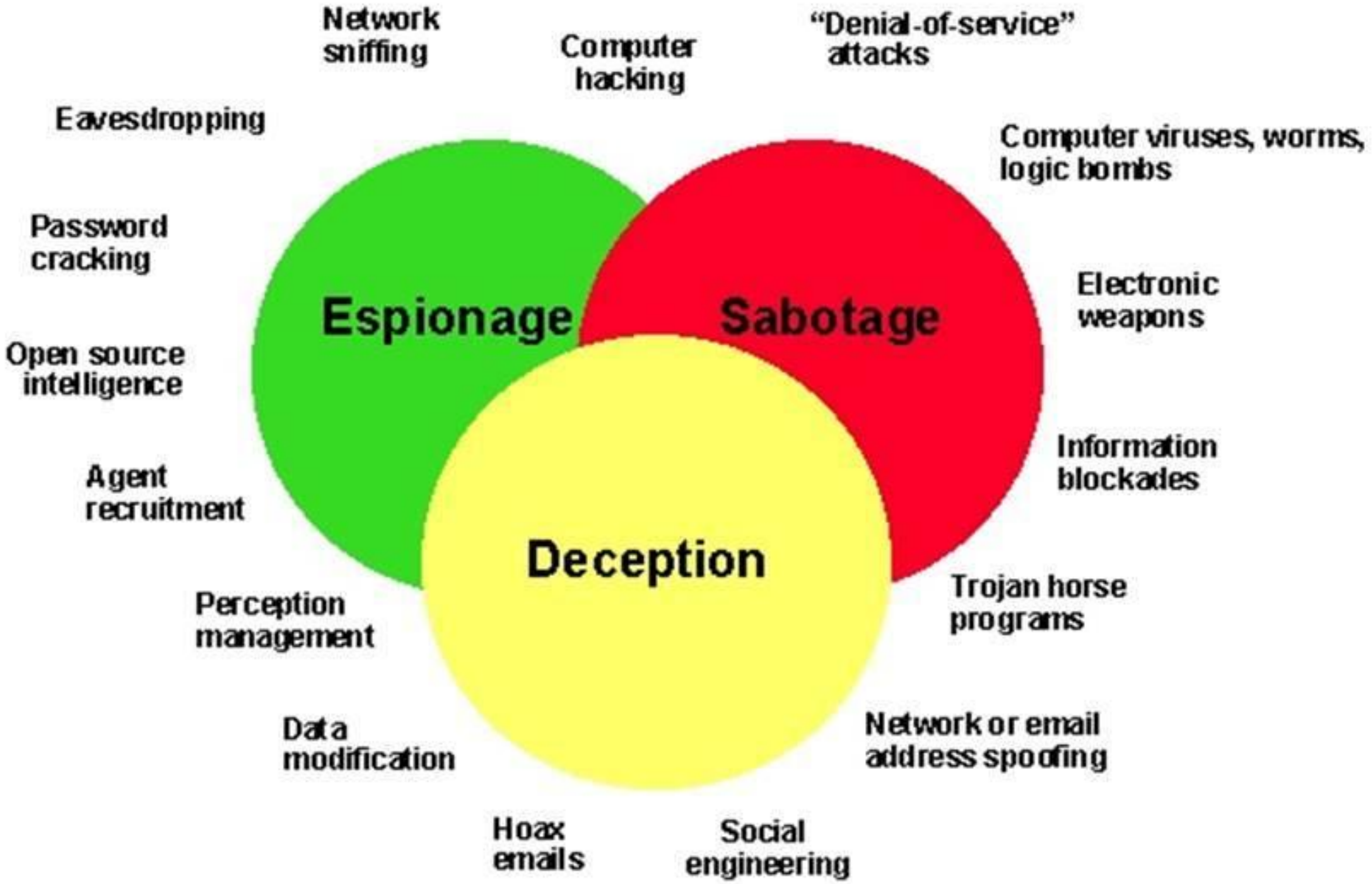
Approx. 30,000 hectares
Contaminated by explosives

Source: Munich Security Report 2016

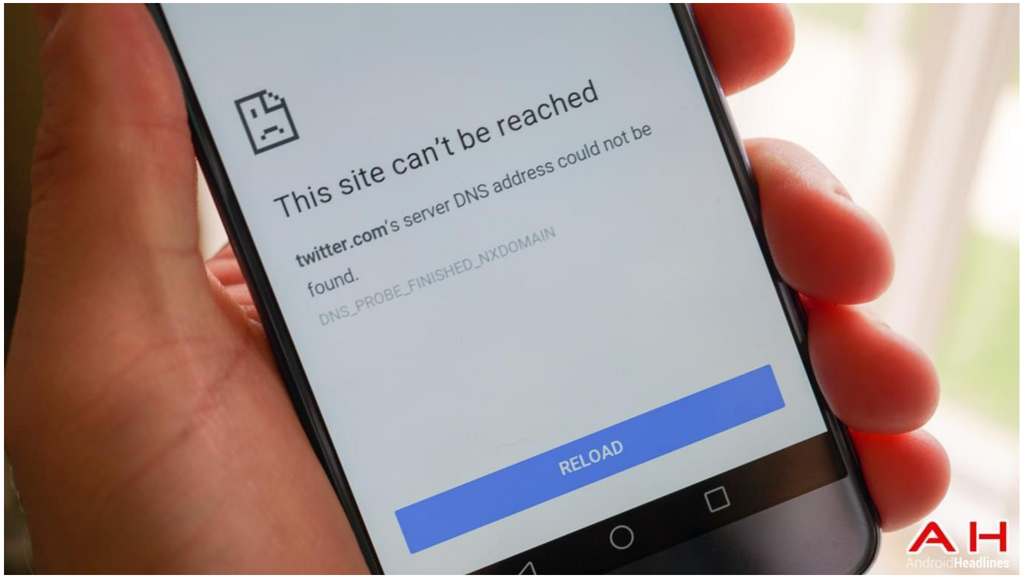
Part 2:

A Survey of Russian Cyber and Information Warfare in Ukraine

Intersection of cyber and information warfare



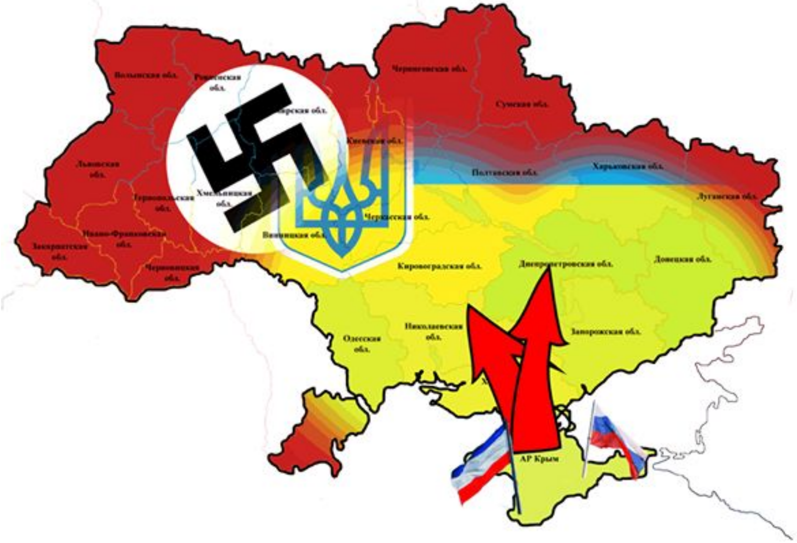
Disrupting government websites



This site can't be reached

twitter.com's server DNS address could not be found.

DNS_PROBE_FINISHED_NXDOMAIN



→ Ukrainian government websites, networks, media and news were the target of *DDoS* attacks and *website defacement*

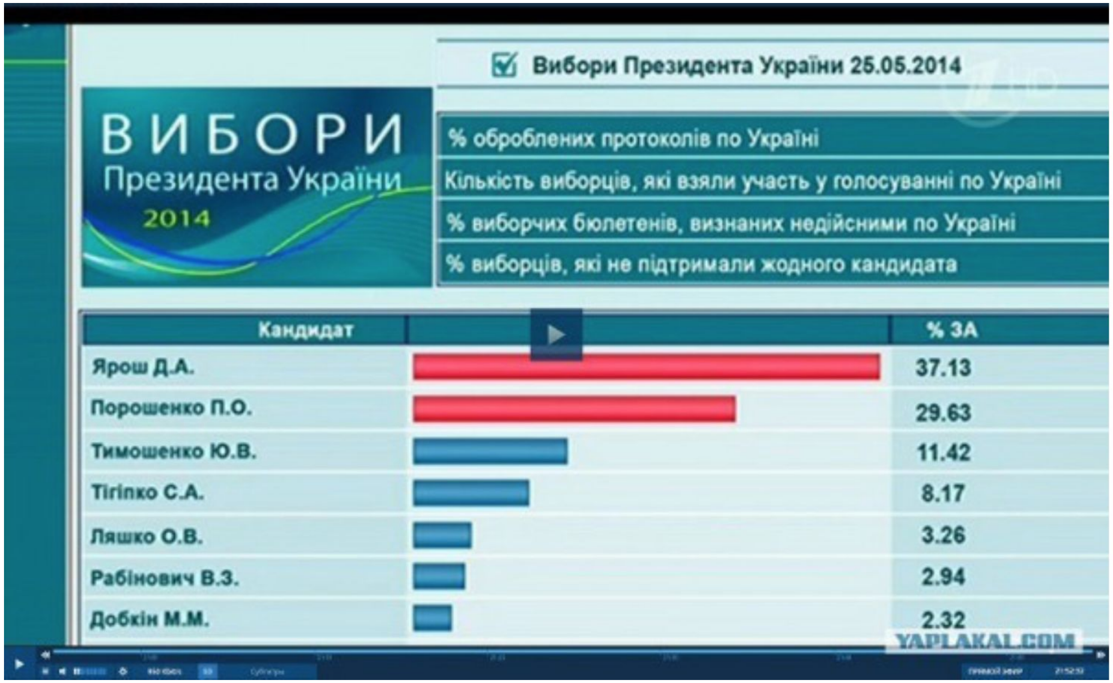
Hacking the election

May 24, 2014

Ukraine’s Central Election Commission (CEC) servers are hacked by pro-Russian group named “CyberBerkut”

- Key files deleted

- Malware caught and removed shortly before election results were posted



☑ Вибори Президента України 25.05.2014

ВИБОРИ
Президента України
2014

% оброблених протоколів по Україні

Кількість виборців, які взяли участь у голосуванні по Україні

% виборчих бюлетенів, визнаних недійсними по Україні

% виборців, які не підтримали жодного кандидата

Кандидат	% ЗА
Ярош Д.А.	37.13
Порошенко П.О.	29.63
Тимошенко Ю.В.	11.42
Тігіпко С.А.	8.17
Ляшко О.В.	3.26
Рабінович В.З.	2.94
Добкін М.М.	2.32

Pro-Kremlin channel announced on the election night that a far right politician Dmitro Yarosh is the leader of the first round of the presidential elections in Ukraine

Attacks on critical infrastructure: Ukraine Power Grid

December 23, 2015

Cyber attacks cause power outages at three Ukrainian transmission stations impacting 225,000

- First cyber attack on a state's power grid
- Coordinated attack within 30 minutes
- Remote access allowed attackers to control and operate breakers
- Call centers targeted with *DoS* attacks

- *BlackEnergy3*
- *KillDisk*

Russia’s “Little Green Men”

Armed fighters without insignias appear in Crimea with no attempt to mask their Russian accent or weapons

Russian media refer to them as “friendly people” who were “good to civilians”

Western media hesitates to acknowledge that they are Russian troops

Malaysian Airlines flight MH17

- On July 17, Malaysia Airlines' flight MH17 from Amsterdam to Kuala Lumpur is shot down by combatants in Ukraine resulting in approximately 300 dead.
- It was flying on an authorized route, at a normal altitude, in regular contact with air traffic controllers until a ground-to-air missile suddenly destroyed it.
- In May, Russia began to supplying anti-aircraft missiles and the teams that operated them to pro-Russian separatists in the Donbas

- Major Russian channels blamed a Ukrainian missile or Ukrainian aircraft, and claimed that the real target had been the President of Russia
- **The following day, Russian spread additional versions of the event:**
  - Ukrainian air traffic controllers instructed MH17 to reduce their altitude
  - A Ukrainian fighter aircraft had been on the scene
  - Ukrainian forces had shot it down during training exercises
  - Igor Girkin (Stelkov) claimed Russia had indeed shot down MH17-- but the CIA had filled the plane with corpses to provoke Russia.

Russia’s information warfare narrative

- Ukrainian dependency on Russia and the inability of the Ukrainian state to provide for its citizens/inhabitants;
- Radicalization of the Ukrainian government and politicians → framing them as fascists
- Threat of security for ethnic Russians and Russian-speakers → justification for the formation of the pro-Russian self-defense groups in East Ukraine;
- Euromaidan is a US/EU satellite and its supporters are traitors;
- The West is “evil” → is preparing extremists to cause public disorder in Ukraine and promotes moral decadence;
- Russia is familiar to Ukraine but Western democracies are strangers →
the common history of Russia and Ukraine, the Orthodox religion as a uniting element

The role of hacktivists and non-state actors

pro-Ukrainian

- Cyber Hunta
- Cyber Hundred
- Null Sector
- Ukrainian Cyber Troops/Army

pro-Russian

- CyberBerkut
- APT 28
- APT 29
- Anonymous Ukraine
- Quedagh
- *Trolls*

Comparison of cyber warfare in Georgia vs. Ukraine

- In December 2016, President Petro Poroshenko said Russian hackers have targeted Ukrainian state institutions 6,500 times over the last two months
- Ukraine has faced repeated attacks on critical infrastructure
- Emergence of more sophisticated *malware*
- BUT: Russian cyber attacks in the Ukraine conflict were not new and did not reach the same level of intensity as the Georgian conflict

Part 3:

Russian Strategy and Rationale

Why hasn’t there been a full-scale cyber war in Ukraine?

Information warfare as superior to cyber warfare

Effectiveness of Russia information warfare in Ukraine

Gerasimov Doctrine

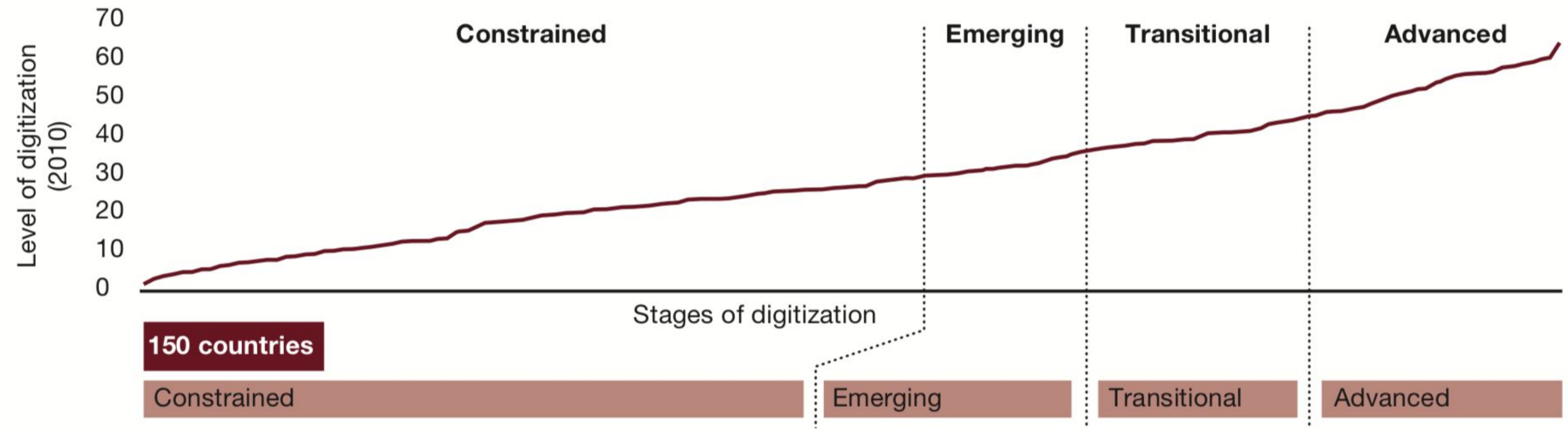
Preconditions for a cyber war

	Capability	No Capability
Vulnerability	Cyber war possible	No cyber war possible
No Vulnerability	No cyber war possible	No cyber war possible

→ **Precondition for a cyber war:** at least one side has the capability to conduct cyber warfare and the other side has enough digitized networks to be vulnerable to cyber attacks

The level of digitalization in Russia and Ukraine

Digitalization Index



65 countries, including: Afghanistan, Kyrgyzstan, India, Cuba, Iraq, Thailand

19 countries, including: Albania, Georgia, Lebanon, Venezuela, China

28 countries, including: Argentina, Mexico, Turkey, **Ukraine**

38 countries, including: USA, most EU countries, South Korea, Australia, **Russia**

→ **Both Russia and Ukraine have:**

- comparatively technologically advanced societies
- a strong information technology (IT) base
- plenty hackers

Source: Booz & Company, World Economic Forum

Possible reasons for the absence of a full-scale cyber war

1. **Ukraine does not have enough loyal hackers**
2. **Neither Russia nor Ukraine has valid targets**
3. **There is no need – the Russians already own Ukraine**
4. **Neither Russia nor Ukraine wants such an escalation**
5. **Cyber war is not a “silver bullet“**

Information warfare rather than cyber warfare!

„Information is now a species of weapon“ **– Russians Maj. Gen. (R) I. Vorobyev and Col. (R) V. Kiselyov**

- in Russian tactical thinking information has been understood to be a form and source of great power long before the inception of the Internet and the cyber space
- → **Russia has not changed its strategy but only its tactics**
- In Russian strategic and military thinking information can be used to
  - disorganize governance,
  - organize anti-government protests,
  - delude adversaries,
  - influence public opinion,
  - and reduce an opponent's will to resist
- such activities can begin prior to the onset of traditional military operations
- → **Russia feels under attack from information warfare from the West ever since the Cold War**

Why is Russian information warfare in Ukraine so effective?

- Russian-language friendly social media (e.g. Vkontakte and Odnoklassniki) can be controlled from Russia and have their HQs there
- many in the Former Soviet Union are naturally skeptical of mainstream information channels → word of friends and colleagues is immeasurably more important than that of mass media
- rise in the quantity and level of sophistication of professional ‘trolls’ and ‘opinion agents’ in Russia
- Russia and Ukraine share largely a common language (Russian)
- is technically less constraint than ”conventional” cyber warfare methods: usually does not require subverting computers through the discovery of vulnerabilities or the engagement of exploits

Not the end of the story!?

- Similar to the frozen conflicts, the long-term goal is not necessarily to prevail but to keep the region destabilized
- Russians have an extensive knowledge of Ukrainian systems → most of Ukraine’s infrastructure is well understood – if not designed by – Russian enterprises
- sufficient number of insiders in Ukraine who are friendly to Russia: could either be bribed or blackmailed into leaking sensitive government materials, disseminating propaganda, installing malicious software, or even physically destroying key systems

The bigger picture: Russia‘s Gerasimov Doctrine?

“The very ‘rules of war’ have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. […] All this is supplemented by military means of a concealed character.”

– Valery Gerasimov, Chief of the Russian General Staff

- Many in the West believed this to be the best articulation of the Russian strategy
- However, Gerasimov was actually talking about how the Kremlin understands what happened in the “Arab Spring” uprisings, the “color revolutions” against pro-Moscow regimes in Russia’s neighborhood, and in Ukraine’s “Maidan” revolt
- Russia has a broad political objective: distract, divide, and demoralize
- But the means to achieve this are largely opportunistic, fragmented, even sometimes contradictory
- implying a military-led campaign and one with coherence and tight command, it also leads us to misunderstand the threat and miscalculate the response

Part 4:

Conclusions and Discussion

Conclusions

- chief objective of Russia’s information warfare strategy is to cause distraction and confusion → conflict in Ukraine can be seen as a textbook example for that
- however, Russian cyber and information warfare in Ukraine is a special case both in terms of capabilities and vulnerabilities
- cyber as a means to an end for information warfare
- Russian doctrine envisions continuous informational attack in peacetime and wartime alike
- dominant theme of the Russian narrative pushed through its information channels is positioning a Slavic Orthodox Civilization in opposition to a “decadent” and morally declining Europe
- one of the main reason for why Russia conducts information warfare is that it feels also to be under attack by the West

What keeps us up at night?

Information warfare!

- relatively easy to disseminate false information and to conduct “information warfare”
- but very difficult to counter false information

Sources:

Baezner, M., & Robin, P. (2017). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict* (CSS Cyber Defense Project). Zurich: Security Studies (CSS), ETH Zürich. Retrieved from http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf

Booz & Company. (2012). *The Global Information Technology Report 2012: Living in a Hyperconnected World*. World Economic Forum.

Central Intelligence Agency. (2018). The World Factbook. Retrieved May 24, 2018, from https://www.cia.gov/library/publications/the-world-factbook/geos/up.html

Galeotti, M. (2018). I'm Sorry for Creating the 'Gerasimov Doctrine.' *Foreign Policy*. Retrieved from http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Giles, K. (2015). Russia and Its Neighbours: Old Attitudes, New Capabilities. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 19–28). Tallinn: NATO CCD COE Publications.

Jaitner, M. L. (2015). Russian Information Warfare: Lessons from Ukraine. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 87–94). Tallinn: NATO CCD COE Publications.

Kerckhoff, E. (2017). Russia's Near-Abroad Interventions: Crazy Like a Fox. *Canadian Military Journal*, *17*(4).

Korsunskaya, D. (2014, November 20). Putin says Russia must prevent "color revolution." *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-putin-security/putin-says-russia-must-guard-against-color-revolutions-idUSKCN0J41J620141120

Sources:

Koval, N. (2015). Revolution Hacking. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 55–58). Tallinn: NATO CCD COE Publications.

Libicki, M. C. (2015). The Cyber War that Wasn't. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 49–54). Tallinn: NATO CCD COE Publications.

Maurer, T. (2015). Cyber Proxies and the Crisis in Ukraine. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 79–86). Tallinn: NATO CCD COE Publications.

Munich Security Conference. (2017). Munich Security Report 2017. Retrieved November 18, 2017, from https://www.securityconference.de/de/debatte/munich-security-report/

Pakharenko, G. (2015). Cyber Operations at Maidan: A First-Hand Account. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 59–66). Tallinn: NATO CCD COE Publications.

Ring, T. (2015). *Russian Information Operations and the Rise of the Global Internet*. University of Washington, Seattle, WA.

Smolaks, M. (2014). Ukrainian Security Service Claims Politicians' Phones Are Under Attack. Retrieved May 24, 2018, from https://www.silicon.co.uk/workspace/security-service-ukraine-claims-politicians-phones-attack-140643?inf_by=5b05040a671db8ef128b51fd

Snyder, T. (2018). *The road to unfreedom : Russia, Europe, America* (First edition.). New York, NY: Tim Duggan Books.

The Federal Government of Germany. (2018). Ceasefire over Easter. Retrieved May 24, 2018, from https://www.bundesregierung.de/Content/EN/Artikel/2018/03_en/2018-03-29-ukraine-osterwaffenruhe_en.html;jsessionid=974E82C30CCD68A82218B357FC5EE53F.s6t1