RUSSIAN CYBER STRATEGY AS PART OF FOREIGN POLICY

WHAT YOU NEED TO KNOW

2 MAIN POINTS

- Russian cyberwarfare policy is not entirely NEW, but is rather a continuation of existing strategies and tactics
- New domain offers advantages in use of key 'traditional' Russian capabilities – including information warfare, active measures, propaganda
- NOT useful to think of Russian cyber measures as SEPARATE from traditional warfare capabilities – rather integrated into traditional forms of warfare, in which cyber domain can act as a force multiplier
- NEW forms of warfare are cheaper and faster, and conflicts are thus sped up

3 CYBER IS NOT REALLY A NEW DOMAIN, PART OF HISTORIC EMPHASIS ON:

- Capturing and controlling the narrative
- Utilization of information resources – to include disinformation, propaganda and psychological operations
- *Existential nature of struggle means that they are not seeking to establish a Balance of Power in cyberspace, but rather to control it. Will not accept and recognize limits on their activities.*

4

Country	Annual Financing in millions of dollars	Number of Cyber troops
US	7000	9000
China	1500	20,000
UK	450	2000
Russia	300	1000
Germany	250	1000
North Korea	200	4000

Information from Zecurion Analytics, January 2017
*This does not include sub-contractors or private contracts.

5 FROM THE RUSSIAN SECURITY ORGANIZATION "MEDUSA", 2016

- Russia's Ministry of Defense focused some of its earliest efforts on recruiting both from academic institutions and from hackers who may have arisen from the criminal underground.
- - The teams were organized into groups known as "research squadrons," many of which lay within various Russian ministries and military units.
- - Some of Russia's earliest cyberattacks were on nearby Baltic states, dating back to a dispute with Estonia in 2007 over the placement of a memorial statue.
- - Public records show that at least one Russian institution purchased surveillance tools from the private Italian company Hacking Team, which sells products that allow governments to spy on their own citizens.
- - Over time, the Russian government developed its own offensive cyberweapons, and also bought tools from cybersecurity companies that could be used for surveillance and espionage

6 PART ONE: WHAT IS RUSSIA'S CYBERSTRATEGY?

TODAY, RUSSIA BELIEVES

- The cyberdomain is intimately connected with 'real space' and it represents merely another arena for playing out historic conflicts

2017 report, Connell and Vogler:

Russian officials are convinced that Moscow is locked in an ongoing, existential struggle with internal and external forces that are seeking to challenge its security in the information realm.

8 FIFTH DOMAIN AS BATTLEFIELD:

- Anonymity/attribution problem: multiple attack vectors can occur, use of both civilian and military means
- Speed
- Irrelevance of geography

9 INFORMATION OPERATIONS ARE A FORCE MULTIPLIER

- Military generals and analysts refer to use of information technology as "remote engagement"; do not need to be present to engage
- Describes new ways of fighting as asymmetric (cheaper, requires fewer inputs; can be performed by non-state actors; utilization of surprise and non-traditional attacks; advantage is not to defender but to he who acts)

10 GENERAL GERASIMOV, 2013 ARTICLE IN MILITARY THOUGHT

- urged the adoption of a Western strategy that involved military, technological, media, political, and intelligence tactics that would destabilize an enemy at minimal cost.
- in the future, wars will be fought with a four-to-one ratio of nonmilitary to military measures.
- Nonmilitary: efforts to shape the political and social landscape of the adversary through subversion, espionage, propaganda, and cyberattacks.

11 GERASIMOV DOCTRINE

- When faced with the combination of pressure and interference, a "perfectly thriving state can, in a matter of months, and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."

12 2013 ARTICLE IN "MILITARY THOUGHT" BY GENERALS BOGDANOV AND CHEKINOV

- Victory is assured if an opponent's political and economic system is made ungovernable, its population demoralized, and its key military-industrial complexes destroyed or damaged beyond repair.
- Russia seeks INFORMATION SUPERIORITY – to be in forefront of military advances, not copying them (development of quantum computing, etc.)
- Importance of FORECASTING future conflicts and conducting ANTICIPATORY OPERATIONS

13 IMPLICATIONS

- Russia's actions in cyber are OFFENSIVE and PREEMPTIVE vs. Reactive and defensive
- Doesn't accept notion that there is a distinction between MILITARY and CIVILIAN targets; military and civilian forces; seek closer and better integration between the two
- Doesn't consider LOAC and other traditional ways of governing conflict as applicable

RUSSIAN ACTIONS HAVE AND DO:

- Violate sovereignty of other nations (i.e. Seeking to interfere in elections, targeting civilian political officials, releasing private information, political doxing)
- May be preemptive in nature
- Seek to destabilize other nations' and cause citizens to doubt the legitimacy of their regimes and their elections

15 DNC HACK

- "The DNC breach really hits home on the evolution of the data breach from a sort of petty crime or adolescent act of vandalism to a professionalized tool of global influence being deployed by state-sponsored organizations carefully executing these acts in order to influence national elections with international consequences," says Danny Rogers, CEO of the security firm Teribium Labs.

16 PART TWO: SPECIFICS OF RUSSIA'S TACTICS

17 BRANDON VALERIANO: DATABASE OF CYBER CONFLICTS

- Suggests that many cyber conflicts (including Russia-Georgia more closely resemble COVERT ACTIVITY than they do traditional ARMED CONFLICT)
- Covert activities may involve things like outsourcing dirty work to hacktivists, cyber criminals

18 USE OF NONMILITARY METHODS, TO INCLUDE

- Potential of mass demonstrations
- Special forces activities
- Information activities
- Outsourcing of operations to contractors, etc.

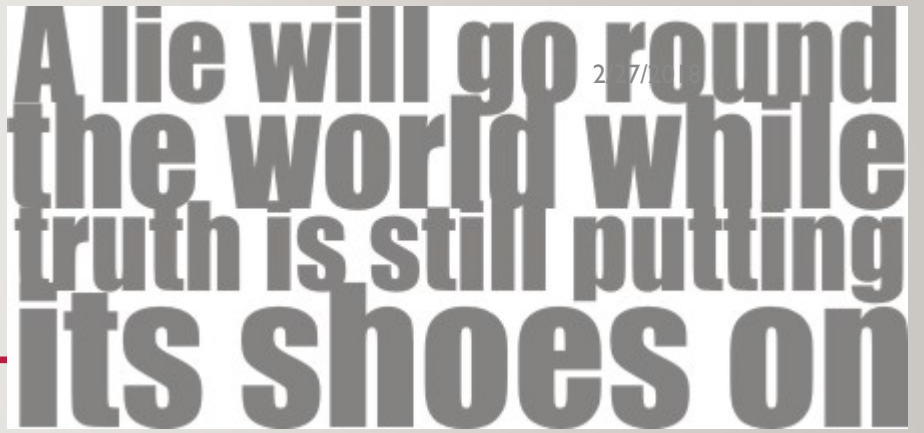
19 KEY TERMS: PROVOCATION

- *Taking control of your enemies in secret and encouraging them to do things that discredit them and help you. You plant your own agents provocateurs and flip legitimate activists, turning them to your side…While this isn't a particularly nice technique, it works surprisingly well, particularly if you don't care about bloody and messy consequences. (John Schindler)*

20 WHAT ARE 'ACTIVE MEASURES'?

- "influencing the course of world events in favor of the Soviet Union, while discrediting and undermining the influence of the United States."
- Sowing conspiracy theories, planting false information in foreign newspapers, getting audiences to believe that their government is lying to them, not sharing information.
- NEW INTERNET ENVIRONMENT good place to continue these traditional Russian strategies and tactics.
- Michael Weiss: "In the current environment, the Kremlin has weaponized money, culture and information."

21 DISINFORMATION



- KGB General Oleg Kalugin:
- Strategy 'to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.'
- **Most common subcategory of active measures**
- "feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister." (Michael Weiss, Soviet analyst)

22 WHAT THIS LOOKS LIKE FOR THE US:

- The election is rigged. #notmypresident.
- The leader is illegitimate. #resist
- The police cannot be trusted. #Charlottesville #blm #Ferguson
- Television lies. #fakenews
- Conspiracy theories: The government PLANNED Parkland massacre in order to implement gun control. Students aren't really students but 'plants' paid by some sinister foreign force.

TROLLING

- Troll: a person who sows discord on social media, by starting quarrels or upsetting people, by posting inflammatory, extraneous or off-topic message in an online community (such as a newsgroup, forum, chat room or blog) with the intent of provoking readers into an emotion response or of otherwise disrupting normal, on-topic discussion, often for the troll's amusement.

24 THE THREAT OF TROLLS

- Internet Research Agency :
- employed more than 600 people across Russia
- implied annual budget of $10m – half of which was paid out in cash.
- Employees were expected to post on news articles 50 times a day. Those who wrote blogs had to maintain six Facebook accounts and publish at least three posts daily. On Twitter, they had to have at least 10 accounts, on which they would tweet 50 times. All had targets for the number of followers and the level of engagement they had to reach.
- Active during US presidential elections. Many people didn't realizing the twitter accounts they followed were fake.

25 IMPLICATIONS OF SOCIAL MEDIA WARFARE

- Difficult to distinguish real from fake news
- Makes ALL news suspect
- Creates a situation where individuals may be less likely to trust ALL news, as well as all government information
- This is problematic when mobilizing citizens to evacuate, etc. In a situation of natural disaster or other threat

26 IMAGINE WHAT THEY COULD DO WITH THIS:

- https://www.youtube.com/watch?v=H153u186OGE

27 RECENT REPORT FROM RAND CORPORATION: "TRUTH DECAY"

TREND	EXAMPLE
Increasing disagreement about facts and analytical interpretations of facts and data	Controversy over safety of vaccines, trends regarding criminality in US, climate change
Blurring of lines between opinion and fact	"News page columns" in New York TImes
Increasing volume and importance of OPINION and PERSONAL EXPERIENCE over fact	Personal interest stories (i.e. one immigrant's experience, DACA, etc.) taking up increased percentage of news
Declining trust in formerly respected sources of factual informaiton	Significant drops in public confidence and trust in government, newspapers, television news, books, the judiciary, and the presidency, as indicated by polls

28 PART THREE: LOOKING TOWARDS THE FUTURE

- 

29 FUTURE THREATS: I AI-ENABLED CYBER ATTACKS

- Artificial intelligence (AI) will be used to:
- Better gather and aggregate information to be used in spear-phishing attacks; access multiple databases and share information between them
- Better identify targets who would be likely to respond to spear-phishing

"AI will make existing cyber attacks efforts – like identity theft, DDoS attacks and password cracking – more powerful and more efficient."

30 READ MORE

Routledge.
2018
Available through Amazon