



Information Warfare... Not just another buzz-word

Eric Stride

estride@deloitte.com

Presentation for DAFITC, Aug 29-31, 2022

**THIS IS A DRAFT SLIDE PRESENTATION AND IS
NOT READY FOR USE**

IT IS SUBMITTED FOR REVIEW ONLY

**THE FINAL VERSION OF THE SLIDES WILL BE
PROVIDED AT/PRIOR TO THE EVENT**

**PLEASE NOTE THAT THE FINAL VERSION WILL
LIKELY INCLUDE CHANGES TO THE SLIDES TO
MAKE THEM:**

- More visually appealing
- Contain less words
- Combine some slides of similar content
- Expand on content of audience interest
- Consistent with theme

The Buzz-Word Crypt

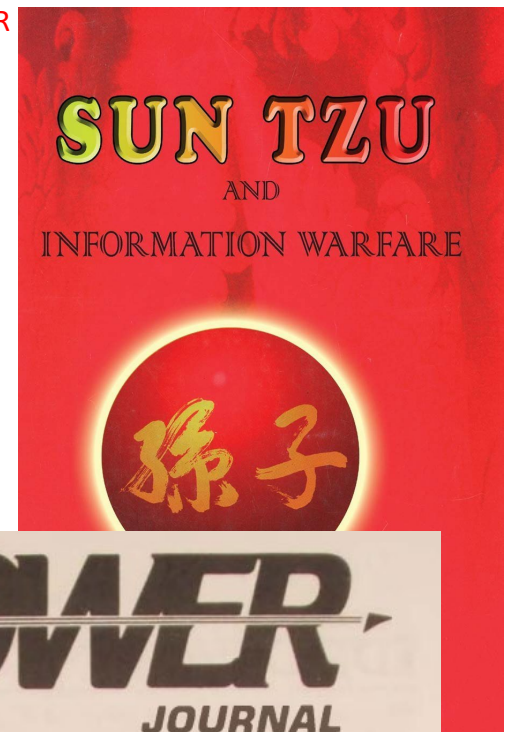


- Network Warfare -> Cyberspace Operations
- Psyops -> MISO
- Computer Network Attack -> Offensive Cyber Operations
- Computer Network Defense -> Defensive Cyber Operations
- Electromagnetic Warfare -> Electromagnetic Spectrum Operations
- Information Operations
- Information Warfare

Who am I... why am I up here?

- 20+ years experience in Cyber, IO, ISR, IW
 - 12 years on Active-Duty
 - 8 years in the Reserve
 - 8 years in the Private Sector
 - Information Operations Squadron in 2005
 - Network Warfare Squadrons (2006, 2012, 2021)
 - Intel Squadron in 2009
 - 2x Commander (1x Det, 1x Sq)
 - NAF-level Support (8th Air Force; 24th Air Force, then 16th Air Force – the IW NAF)
- 5 years at NSA
 - CNODP Grad / Capabilities Developer
 - RIOT Grad / Interactive Operator
 - Deputy Chief of TAO at NSA-Georgia
- First Team Lead for 105 CMT for USCYBERCOM
- Civilian Experience
 - SVP at a Cybersecurity Company
 - Capability Development
 - Advanced Cyber Training
 - CTO at a Cybersecurity Startup
 - Independent Cybersecurity Consultant
 - Specialist Executive w/ Deloitte

Information Warfare (IW)... Is It New?



- 500 BC: Sun Tzu
 - “What is of supreme importance in war is to attack the enemy's strategy.”
 - Robert Neilson's 1997 book
- IW in the Air Force
 - 1995: “information warfare is about the way humans think and, more importantly, the way humans make decisions.”
 - 1995: “any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.”
 - Lots Between, but I only have 50 minutes
 - 2019: Standup of 16th Air Force

AIRPOWER		
JOURNAL		
Spring 1995	Vol. IX, No. 1	AFRP 10-1
FEATURES	STRATEGY AND POLICY	
	State of the Air Force	4
	Dr Sheila Widnall, Secretary of the Air Force	
	The Enemy as a System.....	40
	Col John A. Warden III, USAF	
	INFORMATION WARFARE	
	Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos	15
	Chris Morris, Janet Morris, Thomas Baines	
	Information Warfare	30
	Prof George J. Stein	
	A Theory of Information Warfare: Preparing for 2020	56
	Col Richard Szafranski, USAF	

Is IW New for our Adversaries?

China

- 500 BC: Sun Tzu – basis for Sun Ping's Military Methods
- 1995: Maj Gen Wang Pufend – founding father of Chinese IW
- 1999: War Without Limits – PLAAF Senior Colonels Qiao Liang & Wang Xiangsui
- 2002: PLA's IW strategy spearheaded by Maj Gen Dia Qingmin

So What is IW?

- Is it Cyber? Is it ISR? Is it EW? Is It PA? Is it Weather?
- How is IW different than Information Operations (IO)?

IW is...

- Information Warfare: the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict.
- Short version: consistently and persistently target the adversary's human and system behavior and decision-making
- The six principal AF IW capabilities include:
 - Intelligence, Surveillance and Reconnaissance (ISR)
 - Information Operations (IO)
 - Cyberspace Operations (CO)
 - Electromagnetic Spectrum Operations (EMSO)
 - Public Affairs (PA)
 - Weather (WX)
- There are numerous other information capabilities and organizations that inform and support the employment of these six principal capabilities.

Key Terms

- **Information Advantage:** the product of situational understanding, the ability to assure and exchange information, make and communicate decisions by maintaining advantages in all domains.
- **Decision Advantage:** the product of situational understanding, the ability to assure and exchange information, make and communicate decisions by maintaining advantages in all domains.
- **Convergence:** the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes. Convergence generates outcomes greater than each individual capability can create on its own.

Why do we need IW?

- IW capabilities are the foundational information building blocks to enable operations and airpower execution.
- IW capabilities and integration support the Joint Force Commander's intent by achieving the **information advantage** and **decision advantage**.
- The combination, synchronization, and deliberate integration of IW capabilities allows the USAF to
 - ***generate insights*** (indications and warning, intelligence, situational understanding)
 - ***compete now*** (expose competitor and adversary's actions (counter malign influence/reduce plausible deniability), persistently engage, defend forward)
 - ***set conditions*** for conflict (readiness, proficiency)

Why IW “Stumbled” Previously

- Overshadowed by kinetic ops
- Not “trusted” to achieve the outcomes
- Too Early
- Behind the “green door”
- Cyber “fairy dust”

Why a “Resurrection” of IW

- Society, Technology, and the Military have changed!
- Information = the 7th Joint Function in 2017
 - The management and application of information; information’s deliberate integration with other joint functions to influence relevant-actor perceptions, behaviors, and action or inaction; and information’s role in supporting human and automated decision making.
- IW strategy is nested within
 - National Defense Strategy (NDS)
 - Joint Warfighting Concept (JWC)
 - Joint Concept for the Information Advantage (JCIA)
 - Secretary of the Air Force’s Operational Imperatives (OIs)
 - The Chief of Staff of the Air Force’s Accelerate or Change Action Orders (AO)
- IW is a precondition for all five air force core missions – air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control.
- Joint All Domain Operations

IW vs Ops in the Info Environment (OIE)

- Information Environment — The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information.
 - (Draft JP 3-04, Pending Approval)
- IW focuses on the synchronization and integration of IW capabilities, while OIE focuses on military activities.
- Information Warfare: the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict.
- **Operations in the information environment** are described as the *sequence of activities* that use information to affect behavior by informing audiences; influencing external relevant actors; and affecting information, information networks, and information systems.

The AF & OIE

- The Vision
 - USAF provides a force which can drive behaviors of relevant actors across the competition continuum. Information is a foundational element of Air Force activities and military strategy.
- Identified 29 “challenges & opportunities” to seize & shape the IE
- 3 LOEs
 - USAF-wide Implementation: Service-wide Impact; USAF-wide education & training; revised doctrine & policy; org restructuring; guidance on joint and WOG approach to OIE
 - Information Specialization: develop info professional in BOTH technical and social sciences
 - Programs & Technology: Arm Airmen w/ tools and capabilities for msn success

OIE Strategic Challenges and Opportunities

1. Reactive in the Information Environment
2. Risk of Inaction
3. Process Incompatibility
4. Going Nowhere Fast
5. OPSEC Fatigue
6. Data Overload
7. No Way to Assess Impact
8. Plays Well with Others
9. Coherent Guidance
10. USAF OIE Needs a Hero
11. Stovepipes
12. Tangled in Red Tape
13. Over-Classification
14. No Whole-of-Government Approach
15. Crystal Ball
16. Subject Matter Experts
17. The Personal Touch
18. Practical Training
19. No Pipeline to OIE Expertise
20. New Dogs, Old Tricks
21. Words Matter
22. You Are What You Pay For
23. Carpe Diem
24. Know Your Audience
25. Know Your Enemy
26. Inconsistent Narrative
27. The Innovative Force
28. Kinetic Tunnel Vision
29. American Values

Department of Defense

ONLY

DoD Strategy for OIE released	Chairman of the Joint Chiefs of Staff (CJCS) designates information as 7th Joint Function	- National Defense Authorization Act (NDAA) directs Information Operations integration - NDS seeks competition and information advantage	Joint Requirements Oversight Council releases memorandums (JROCM) on JCOIE and JC-HAMO	- NDAA Principal Information Officer Adviser established - Information Cross Functional Team (CFT) forms
2016	2017	2018	2019	2020
14F Air Force Specialty Code (AFSC) established	- Under Secretary of the Air Force (USecAF) Donovan tasks OIE Assessment - USAF IW Tiger Team forms	- Tiger Team delivers outbrief to USecAF Donovan - VCSAF signs charter to designate OIE Tiger Team Authority - FY18 funds awarded for USAF OIE Assessment	- Tiger Team visits PACAF and USAFE for OIE Assessment 16th Air Force activates - USAF OIE Strategic Imperative White Paper published - USAF completes OIE Assessment and Report - VCSAF pens memo: "I'm excited about our USAF OIE efforts but want to move faster to deliver outcomes." - Tiger Team creates first OIE Implementation Plan draft	- OIE Implementation Plan activities coordinated at 3-digit HAF / 2-digit MAJCOM - C2 of OIE Report v1 published - OIE FY22 Program Objective Memorandum input - OIE CFT transforms into IW CFT - IW MAWG established - IW Operating Concept v0.3 released

USAF

Figure 2: OIE Timeline

OIE Strategic Plan Phased Timeline

- FY22: Establishment of foundational guidance
- FY23: Development of organizational structures and detailed policies
- FY24+: Development of specialist education/training and advanced capabilities
- Identifies “achieve now” activities, with existing resources
 - DOTMLPF-P (w/o the “F”)
 - Aligned to LOE and FY (Initiation / Completion)
 - Names OPRs, recommends OCRs

Sample of OIE Strategy Activities

This slide has overlapping builds and will not look correct if printed

FY22	FY23	FY24+	LOE	OPR	Activity Description	FY22	FY23	FY24+	LOE	OPR	Activity Description & Suggested OCRs
					1. Doctrine						5. Leadership and Education
			1	AF/A3	1.1 Incorporate OIE approaches in level planning, execution, and assessment <i>Proposed</i>						5.1 Identify resourcing requirements to pursue information-related updates to USAF education and training in conjunction with associated joint concepts: In consideration of occupational specialties, positions and time in career; identify, develop, and provide, as appropriate, initial, sustainment and pre-deployment individual and unit training that provides an overview of general and (as appropriate) Area of Responsibility-specific human aspects and elements.
					2. Organization						<i>Proposed OCRs: AF/A2/6, AF/A3, ACC, AFMC</i>
			1	AF/A3	2.1 Establish USAF-level information processes with cross-functional teams to shape operations, activities, and and Combatant Command (CCME) <i>Proposed OCRs: AF/A</i>				1	AETC	6. Personnel
					3. Training				2	AF/A3	6.1 Conduct a full 14F sustainability and talent management analysis. <i>Proposed OCRs: AF/A1, AFRC, NGB</i>
			2	ACC	3.1 Develop a specialized training Airmen on intermediate and advanced						7. Policy
					4. Materiel				1	AF/A3	7.1 Update and revise the OIE Strategic Plan on a five-year or as-needed recurring basis. <i>Proposed OCRs: AF/A2/6, A5/7, SAF/PA, ACC, AFSOC</i>
			2	SAF/PA	4.1 Assess sufficiency of the USAF to maintain an information advantage <i>Proposed</i>				1	AF/A3	7.2 Develop and implement a communication strategy to outline how the 14F community is organized, trained, and equipped. <i>Proposed OCR: SAF/PA</i>
			2	AF/A2/6	4.2 In coordination with the intelligence plan of action and milestones to inform adversary strategies and capabilities strategic vision for OIE, plans, information (IRCs), and level of investment in IRCs. <i>Proposed OCRs: AF/A3, AF/A5/7, MAJCOMs, Partners/Allies</i>				1	AF/A2/6	7.3 Consistent with the Principal Information Operations Advisor's (USD (Policy)) strategy for OIE and DoD policy, integrate OIE processes and IW capabilities into USAF policy and create new policy as needed. <i>Proposed OCRs: AF/A3, AF/JA, ACC, AETC</i>

IW Strategy

- **Vision:** Air Force provides Information Warfare professionals, capabilities, and systems that enable the Joint Force to win decisively across the competition continuum.
- **End State:** Information Warfare capabilities seamlessly integrated into strategic, operational, and tactical planning and execution to deliver converged, cross-domain effects
- Phased timeline
- Objs 1-3 and LOES for each OBJ
- Implementation plan to follow

IW Integration & Synchronization

Helps USAF planners to:

- 1) Leverage informational & cognitive means to achieve operational effects
- 2) Leverage operational effects to achieve informational & cognitive effects
- 3) Shape conditions for air operations in the physical environment using informational capabilities
- 4) Influence the perceptions, attitudes, & behaviors of relevant actors

Achieves information advantage by:

- 1) Informing audiences
- 2) Influencing relevant actors
- 3) Attacking, Exploiting, and Denying adversary freedom of action within the IE
- 4) Defending USAF freedom of action within the IE

IW Strategy Objectives & LOEs

1) Organize the Force

LOE 1: Deliver IW Policy, Oversight, and Guidance

LOE 2: Organize Air Force for IW Planning

LOE 3: Identify Requirements

LOE 4: Build and Execute OT&E flight plan

2) Develop the Force

LOE 1: Develop USAF IW Cultural Mindset

LOE 2: Develop USAF IW Tradecraft

LOE 3: Develop IW Leaders

3) Equip the Force

LOE 1: Deliver sensing, analysis, and information sharing capabilities

LOE 2: Deliver coordinated and integration [modular] operational planning tools

LOE 3: Bolster existing capability within the IW disciplines

Phased Timeline

Phase 1 (2022 – 2025):

- 1) Designate lead Deputy Chief of Staff (DCS) for IW
- 2) Designate lead Major Command (MAJCOM) for IW
- 3) Advocate for integrated IW capabilities throughout the USAF Planning, Programming, Budgeting, and Execution (PPBE) process
- 4) Introduce, adopt, and expand IW concepts into Air Force doctrine and professional military and developmental education
- 5) Integrate IW sub-discipline data into the DAF Data Fabric
- 6) Develop guidance, courses, and processes to institutionalize IW integration in operational planning and assessments and at the service level
- 7) Identify IW concepts, gaps, and requirements to inform development the Air Force the Nation Needs (AFNN)

Phase 2 (2025-2029):

- 1) Establish effective IW planning capabilities integrated at the operational level of war
- 2) Coordinate with AF/A8 to determine updated approach to meet USAF IW requirements throughout PPBE process
- 3) Deliver automated and AI/ML-enabled tools to support rapid planning and assessment of IW
- 4) Deliberately develop airmen that comprehend the integrated nature of operations across the physical and information environments

The How of IW & OIE

- Bridging the “silos”
- Data Fusion
- Partnerships
- Target all phases of the OODA loop



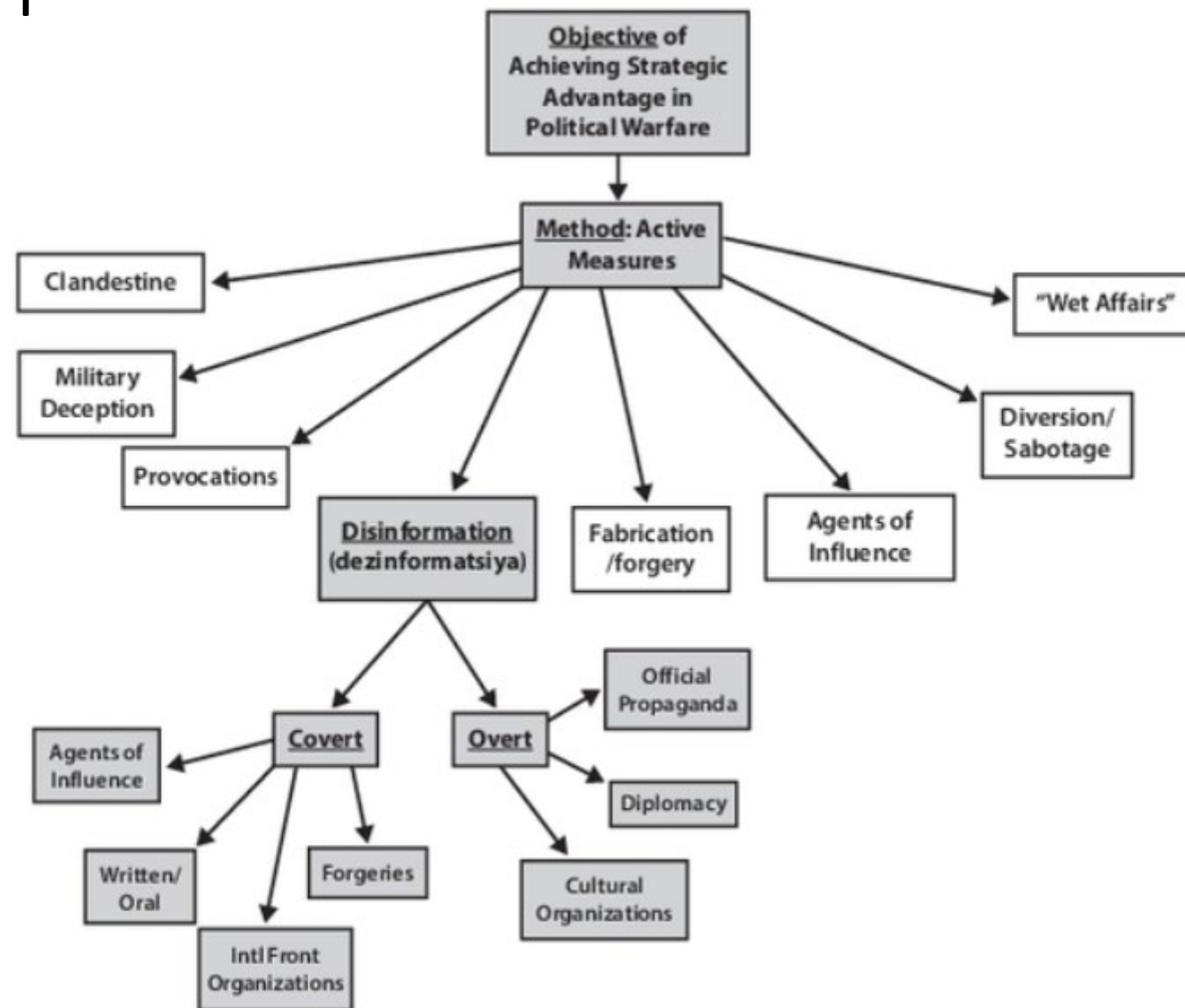
PLACEHOLDER IMAGES FOR
NOW



Adversary IW - Russia

- Already engaged across the spectrum – BELOW the level of armed conflict / use of force
 - Clausewitz: “political warfare”
 - Russian strategists believe they are under siege: Kosovo, EU, NATO
- IW TTPs:
 - Exploiting global social media
 - Controlling Western media outlets
 - Direct lobbying of Western society

Russian “political warfare”



Mis- / Dis- / Mal-Information (MDM)

- **Misinformation** is false, but not created or shared with the intention of causing harm. (Misleads)
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country. (Deceives)
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate. (Sabotage)

Foreign Influence

1. Targeting divisive issues
2. Moving accounts into place
3. Amplifying and distorting the conversation
4. Making the mainstream
5. Taking the conversation into the real world

Examples of IW Operations

- Social Media
 - Example 1
- Western Media Outlets
 - Example 2
- Lobbying of the West
 - Example 3

Election Interference

- In 2016, Russia...
 - Probed state voter databases
 - Hacked the Clinton campaign
 - Hacked the DNC
 - Hacked the Democratic Congressional Campaign Committee
 - Tried to hack the Rubio Campaign
 - Tried to hack the RNC
 - Released politically damaging info on the internet
 - Spread propaganda on Twitter, Facebook, Instagram, and YouTube
 - Staged rallies in FL and PA
 - Set up mtgs w/ members of the Trump Campaign



CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS



Boris Alekseyevich
Antonov



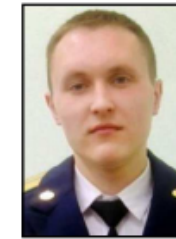
Dmitriy Sergeyevich
Badin



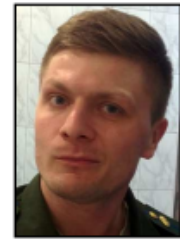
Anatoliy
Sergeyevich Kovalev



Nikolay Yuryevich
Kozachek



Aleksey Viktorovich
Lukashev



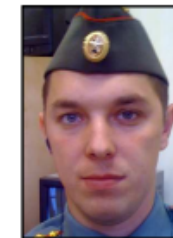
Artem Andreyevich
Malyshev



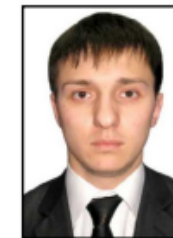
Sergey
Aleksandrovich
Morgachev



Aleksandr
Vladimirovich
Osadchuk



Aleksey
Aleksandrovich
Potemkin



Ivan Sergeyevich
Yermakov



Pavel
Vyacheslavovich
Yershov

DETAILS

On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov, Pavel Vyacheslavovich Yershov, and Viktor Borisovich Netyksho, with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to

Election Defense - 2020

- 2020 Election Defense was #1 priority for NSA & USCYBERCOM
- CISA dedicated significant resources
- Disrupted Russian Troll Farm, IRA
- USCC publicly shared foreign malware samples
- Microsoft and USCC disrupted the TrickBot network
- Social media companies battling bots and fact-checking / labeling
- DHS cybersecurity sensors to election systems in all 50 states and in local election offices in 30 states

IW in the Russian-Ukraine War

- “Reflexive Control”
- Recognizing the Donbass
- “national existential threat” from NATO
- Russian narratives that the war opposes the West, NATO expansion, Nazism, and fascism
- Social media campaigns w/ pro-Russian narratives trending in language groups found in much of South Asia, South Africa, Nigeria, Pakistan, and Iran
 - 35 abstentions, including 17 African countries on UN resolution condemning Russia
- State-run media & false stories, some picked up & ran in other countries (e.g. China)
 - RT stating that “large numbers of Ukrainian soldiers had surrendered
 - Fake reports that Zelenskyy had fled Kyiv
 - Pentagon financing biological weapons in Ukraine

Future of IW

- Scope, scale, and speed of IW will expand
- Will impact the future of conflict
- Will sow disorder, mistrust, and radicalization
 - Could potentially lead to internal strife and violence
- The US military must adapt and integration IW & OIE to defend against our adversaries
 - Across the cognitive, digital, and physical realms
 - Integrate IW into all types of military planning and operations – across the spectrum of conflict
- JADC2

For more information, please contact:

Eric Stride

Specialist Executive

Deloitte & Touche LLP

+ 1 210 390 3278 / + 1 210 542 5449

estride@deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited