

For Public Release



CAB 2021-22/114
February 16, 2022

Modern Information Warfare: Integration of Psychological and Cyber Operations

Modern information warfare¹ poses a serious threat to Western liberal democracies. The People's Republic of China (PRC) and Russia have both restructured their military intelligence organizations to enhance their ability to conduct modern information warfare in what literature from both countries describe as a new domain of warfare: the cognitive domain.² Russia and China conduct modern information warfare, in the cognitive domain, through integration of offensive cyber operations and psychological operations (psyops). This synergy broadens the range of operations that both Russian military intelligence (GRU) and the People's Liberation Army's (PLA) military intelligence information troops³ are able to conduct and support. This integration creates a powerful synergy for information warfare operations within the cognitive domain and complicates our traditional understanding of the operational objectives behind cyber operations, which are often perceived in a limited manner as either espionage or sabotage. By not recognizing the strategic and tactical cognitive domain implications resulting from the integration of psychological and cyber operations in modern information warfare, decision-makers risk being unable to formulate adequately informed policy decisions. Misdiagnosis of the actors' true objectives could lead decision-makers to accept deception as truth and carry out responses that are intended by the adversary. (U// [redacted])

These two authoritarian regimes are using modern information warfare, within the cognitive domain, with the intent to surveil, repress, manipulate, censor, coerce or defeat liberal democracies. Information warfare operations conducted by the GRU and the PLA pose an insidious and serious threat to liberal democracies. [redacted]

¹ **Modern information warfare** is discussed in this paper from the perspective of Russian and PRC doctrines where cyber operations and psychological operations have been integrated into a new operational doctrine for achieving tangible effects in the cognitive domain. Russian and PRC doctrines utilize a holistic understanding of information as a system, incorporating the understanding that almost all information now exists within cyberspace and that the psychology of people is an integral component of information as a system. Within the broader literature there are a range of overlapping terms that describe similar concepts, i.e. cognitive domain operations, information confrontation, cyber warfare, or information operations. Each of these terms generally has a different focal point, a different defined scope of discussion or reflect a different national doctrine. (U)


² The **Cognitive domain** represents the next frontier of warfare domains – land, sea, air, space, cyber and cognitive domains. This domain encompasses the psychology of information processing and the perceptions, attitudes, beliefs and behaviours of people in response to information. Modern Russian and Chinese information warfare doctrines integrate cyber, information and psychological capabilities to achieve their objectives in all domains, including the cognitive. (U)

³ **Information troops** is the term used by the Russian GRU to refer to military intelligence operators in the new combined cyber/psychological organizational structure. [redacted]

Intelligence Assessments Branch
Direction de l'évaluation du renseignement

Canada

For Public Release



Analytical Brief
Précis analytique

CAB 2021-22/114
February 16, 2022

SECRET

Integration of cyber and psyops within modern information warfare operations

[redacted] military cyber operations support three high level objectives: (i) espionage, (ii) sabotage, or (iii) information warfare operations. Integrated cyber-psychological military intelligence operations are used to conduct information warfare in the cognitive domain. (U/[redacted])

Russia and China have both adopted doctrines to conduct information warfare operations in the cognitive domain. These doctrines normalize maintaining a consistent operational tempo that is the same during peacetime and war; one that targets civilians at all times, not just national leaders or militaries, and they employ this capability across all of their geopolitical relationships. Liberal democracies generally draw a sharp distinction between the authorities and types of information operations that are conducted during peacetime vs armed conflict, who they consider to be legitimate targets and the types of mission objectives; Russia and the PRC do not maintain these same distinctions. Their doctrines for modern information warfare operations extend to politics, economy, science, technology, diplomacy, cultural beliefs and individual decision-making and is directed at civilians, politicians, governments, and entire societies across the entire international community. (U/[redacted])

"Foreign politicians talk about Russia's interference in elections and referendums around the world. In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it."

Vladislav Surkov,
Advisor to Russian president Vladimir Putin.
(U)

Modern information warfare has evolved to integrate emerging cyber technologies with psychological techniques to exploit opportunities enabled by the digital age. (U/[redacted])

Russia


In 2017, the Russian GRU formally integrated its cyber and psychological operational organizations, creating what are now known as 'information troops'. The mandate of these information troops is to conduct information warfare operations. Russian special services are actively using cyberspace in their psychological operations to create divisions within Western societies, inter-state relations, and within international organizations, such as NATO. (U)

- *GRU military unit 26165* - The 85th Main Special Service Centre's Unit 26165 had its origins in the 1970s conducting signals intelligence; it has since become the GRU's foremost cyber operations unit. Unit 26165 is publicly referenced as APT28⁴ or Fancy Bear, and is known for cyber operations involving theft of information that is then used in support of psychological operations. It is believed to be responsible for the 'hack and leak' cyber-psychological information warfare operation against the German national parliament in 2015 and the US Democratic National Committee (DNC) in 2016. (U)
- *GRU military unit 74455* - The Main Center for Special Technologies' Unit 74455 represents another element of the GRU's offensive information warfare apparatus. It is a relatively new unit and is linked to some of Russia's most brazen information warfare operations such as the 2017 NotPetya⁵ attack in the Ukraine. Unit 74455 is known for conducting technical information operations that result in the degradation or destruction of their target's computer systems. It is commonly referred to as "Sandworm" among cybersecurity professionals. (U)

⁴ APT28 or Fancy Bear are terms used to identify a group of nation state cyber hackers who operate as part of the Russian (GRU). (U)

⁵ NotPetya is the name of a cyber attack masquerading as ransomware that primarily targeted the Ukraine in 2017. It ultimately spread around the globe and is considered to be one of the most damaging cyber attacks in history. (U)

For Public Release



Analytical Brief
Précis analytique

CAB 2021-22/114
February 16, 2022

SECRET/

- *GRU military unit 54777* - The 72nd Special Service Center (Unit 54777) is the chief psychological operations division within the GRU. It has operated lock-step with GRU hackers since at least 2014, blending cyber operations with psychological operations. Unit 54777 has demonstrated that digital aggression can be carried over into influence operations and the unit has worked alongside GRU's Unit 26165 and Unit 74455 throughout a number of campaigns. (U)


Russian modern information warfare operations

Russia has a holistic approach to its information warfare operations by using cyber operations in coordination with psychological attacks. Such information warfare operations are used to either acquire information or disorganize, disrupt, or destroy a state's capacity to manage its affairs, while psychological operations leverage the cyber components to deceive the victim, discredit the leadership, and disorient and demoralize the population and the armed forces. (U/)

- Russian information operations use a variety of methods to induce a target to make decisions prejudicial to their self-interest. These include distraction, overload, paralysis, exhaustion, deception, division, pacification, deterrence, provocation, suggestion and pressure. These categories of influence can be mutually reinforcing. (U/)
- The concept of *reflexive control* is an additional psychological technique that is sometimes used to manipulate the target into making a decision that is unfavourable to their interests. Use of reflexive control has been documented in multiple Russian geopolitical conflicts. In the realm of information warfare operations, reflexive control exists alongside other forms of 'active measures', including as disinformation (*dezinformatsiya*), penetration (*proniknoveniye*) and provocation (*provokatsiya*). (U)

Examples of likely Russian military intelligence modern information warfare operations


- 2014–2019 Dutch investigation into the downing of Malaysian Airlines flight MH17
 - Objective:
- 2015 France TV5
 - Objective: Open sources indicate that Fancy Bear actors compromised and sabotaged the French television station masquerading as a terrorist organization. Media reporting suggests that this activity was an attempt by Russia to test capabilities against the West while avoiding attribution. Even as a test, the terrorism false-flag was still an attack against the West, likely in line with Russia's overall national objectives to undermine public confidence in Western institutions. (U/)
- 2015, 2016 Ukraine power grid disruption
 - Objective: Cyber attacks likely had the intended psychological effect of undermining the authority of Ukraine's political leadership and its ability to defend the Ukrainian state, while sowing fear that Russia could, at will, remotely disrupt the critical infrastructure of its adversaries. (U/)
- 2015 – 2018 World Anti-Doping Agency (WADA) Russian investigation
 - Objective: In response to WADA's investigation into Russian doping practices, GRU cyber actors compromised WADA in an attempt to discredit allegations against Russian practices and control narratives surrounding any misconduct. (U)
- 2016 US Presidential Election
 - Objective: Russian cyber interference in the 2016 American elections was an attempt to undermine American public faith in democratic processes. (U/)
- 2017 French Presidential Election



Intelligence Assessments Branch
Direction de l'évaluation du renseignement

3 / 6

For Public Release



Analytical Brief
Précis analytique

CAB 2021-22/114
February 16, 2022

SECRET//

- Objective: Similar to the campaigns observed during the 2016 US elections, Russian cyber actors targeted politicians involved in the 2017 French election in an attempt to influence voters and undermine Western democratic institutions. (U// [redacted])

China

The Communist Party of China's (CPC's) information operations are coordinated at a high level within the party state and executed by a range of actors, such as the United Front Work Department (UFWD), The Propaganda Ministry, the State Council Information Office, the PLA and the Ministry of State Security (MSS). In 2016, China began a massive reorganization of the PLA during which the Strategic Support Force (SSF) and its subordinate Network Systems Department (NSD)⁶ were created. (U// [redacted])

- *Network Systems Department* - The NSD incorporates and oversees all strategic operational units operating in the cognitive domain units in the PLA, this includes those responsible for cyber warfare, electronic warfare, psychological warfare and technical reconnaissance. The NSD's information operations include electronic warfare and offensive cyber and psychological operations. (U)

China's operations in the cognitive domain

China's modern information warfare operations use a concept of "Three Warfares", which comprises psychological,⁷ public opinion⁸ and legal⁹ "warfare" operations. China's operations also incorporate concepts of deception and misdirection known as the 36 stratagems. Tactically, China will use psychological techniques of allusion, reasoning and luring to create or disrupt cognitive beliefs of their adversaries, with the intention of diffusing a situation or creating an inability to formulate a coherent policy response. (U// [redacted])

PRC modern information warfare operations are designed to shape international public narratives, weaken the public will of a foreign state, shape diplomatic, political and public narratives and advance China's interests. The use of information operations – encompassing cyber, electronic and psychological operations – is integral to achieving information superiority. (U// [redacted])

Existing examples of likely PRC modern information warfare operations [redacted]

[redacted] (S)

- 2015 Targeting "Great Cannon" against Github¹⁰
 - Objective: In 2015, services designed to circumvent Chinese censorship were disrupted by Denial of Service attacks. Security researchers attribute the attacks to China as part of an attempt to silence public discourse and strengthen acceptance of PRC-approved 'truths'. (U// [redacted])
- 2018 Interference in Taiwan's Election
 - Objective: China's manipulation of social media platforms likely intended to undermine democratic institutions and social cohesion in the PRC-claimed territory. (U// [redacted])
- [redacted] (S)

⁶ The Network Systems Department has also been referred to as the Cyberspace Force in open source literature. (U)


⁷ Psychological warfare uses propaganda, deception, threats and coercion to affect the adversary's decision-making. (U)

⁸ Public opinion warfare disseminates information for public consumption to guide and influence public opinion and gain support from domestic and international audiences. (U)

⁹ Legal warfare uses international and domestic laws to gain international support, manage political repercussions and sway target audiences. (U)

¹⁰ Github is a provider of internet hosting and is commonly used to host open-source software projects. (U)

For Public Release



Analytical Brief
Précis analytique

CAB 2021-22/114
February 16, 2022

SECRET/

- Objective:
- 2020 Indian Border Tensions
 - Objective: Media reports indicate that PLA units targeted Indian government, information technology and banking websites during a time when India and China were engaged in border disputes. The incidents involved data theft
- 2021 Targeting of Uyghurs using Facebook
 - Objective: China actively conducts surveillance operations across social media platforms in order to control messages that are contrary to party objectives. State-sponsored actors have created fake accounts on Facebook, for example, to target Uyghurs living outside China, including individuals in Canada. These tactics undermine democratic values, state sovereignty, and can be used to instill fear in vulnerable populations. (S)

Outlook and Impact to Canada

The PRC and Russia have many tools in their foreign policy arsenal for promoting their national interests by conducting political warfare to influence foreign countries, including information warfare operations discussed herein. (S)

Threat actors who are active in the cognitive domain attempt to weaken democracies by promoting their own narratives and alter the attitudes and beliefs of political leaders and the public. As a result, unless adequately mitigated, our adversaries' narratives or 'versions of the truth' may begin to permeate and dominate Canadian public opinion.

For Public Release



Analytical Brief
Précis analytique

CAB 2021-22/114
February 16, 2022

SECRET

 CSIS_PUBLICATIONS / SCRS_PUBLICATIONS
CANADIAN PARTNERS


THIS INFORMATION IS SHARED WITH YOUR ORGANIZATION FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS DOCUMENT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED IN WHOLE OR IN PART WITHOUT THE WRITTEN PERMISSION OF CSIS. THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO EXEMPTIONS UNDER THE FEDERAL ACCESS TO INFORMATION ACT OR PRIVACY ACT OR UNDER APPLICABLE PROVINCIAL OR TERRITORIAL LEGISLATION. IF A REQUEST FOR ACCESS UNDER THESE ACTS IS MADE, THE RECEIVING AGENCY MUST CONSULT CSIS IN RELATION TO APPLYING THE AVAILABLE EXEMPTIONS. FURTHER, CSIS MAY TAKE ALL NECESSARY STEPS UNDER SECTION 38 OF THE CANADA EVIDENCE ACT OR OTHER LEGISLATION TO PROTECT THIS INFORMATION. IF YOU LEARN THAT THIS INFORMATION HAS OR MAY BE DISCLOSED, THAT THESE CAVEATS HAVE NOT BEEN RESPECTED OR IF YOU ARE UNABLE TO ABIDE BY THESE CAVEATS, INFORM CSIS IMMEDIATELY.

FOREIGN PARTNERS

YOUR AGENCY'S USE OR DISCLOSURE OF THIS INFORMATION MUST BE IN ACCORDANCE WITH INTERNATIONAL HUMAN RIGHTS LAW, INCLUDING THE CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT.

NO LETHAL ACTION MAY BE TAKEN ON THE BASIS OF THIS INFORMATION.

THIS INFORMATION IS FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS INFORMATION MAY BE SHARED WITH MEMBERS OF YOUR GOVERNMENT WHO POSSESS THE REQUIRED SECURITY CLEARANCE AND A NEED TO KNOW. IT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED, IN WHOLE OR IN PART, TO ANY OTHER GOVERNMENT OR ENTITY WITHOUT THE WRITTEN PERMISSION OF CSIS. IF YOU LEARN THAT THE DOCUMENT HAS BEEN IMPROPERLY DISCLOSED OR DISSEMINATED OR IF YOU ARE UNABLE TO ABIDE BY THE CAVEATS IN THIS DOCUMENT, INFORM CSIS IMMEDIATELY.



Intelligence Assessments Branch
Direction de l'évaluation du renseignement

6 / 6