XII Jornadas STIC CCN-CERT
Ciberseguridad,
hacia una respuesta y disuasión efectivas

GRU
Estructura y capacidades ciber

ccn-cert
centro criptológico nacional

- Antonio VILLALÓN HUERTA
- S2 Grupo
- antonio.villalon@s2grupo.es

Índice

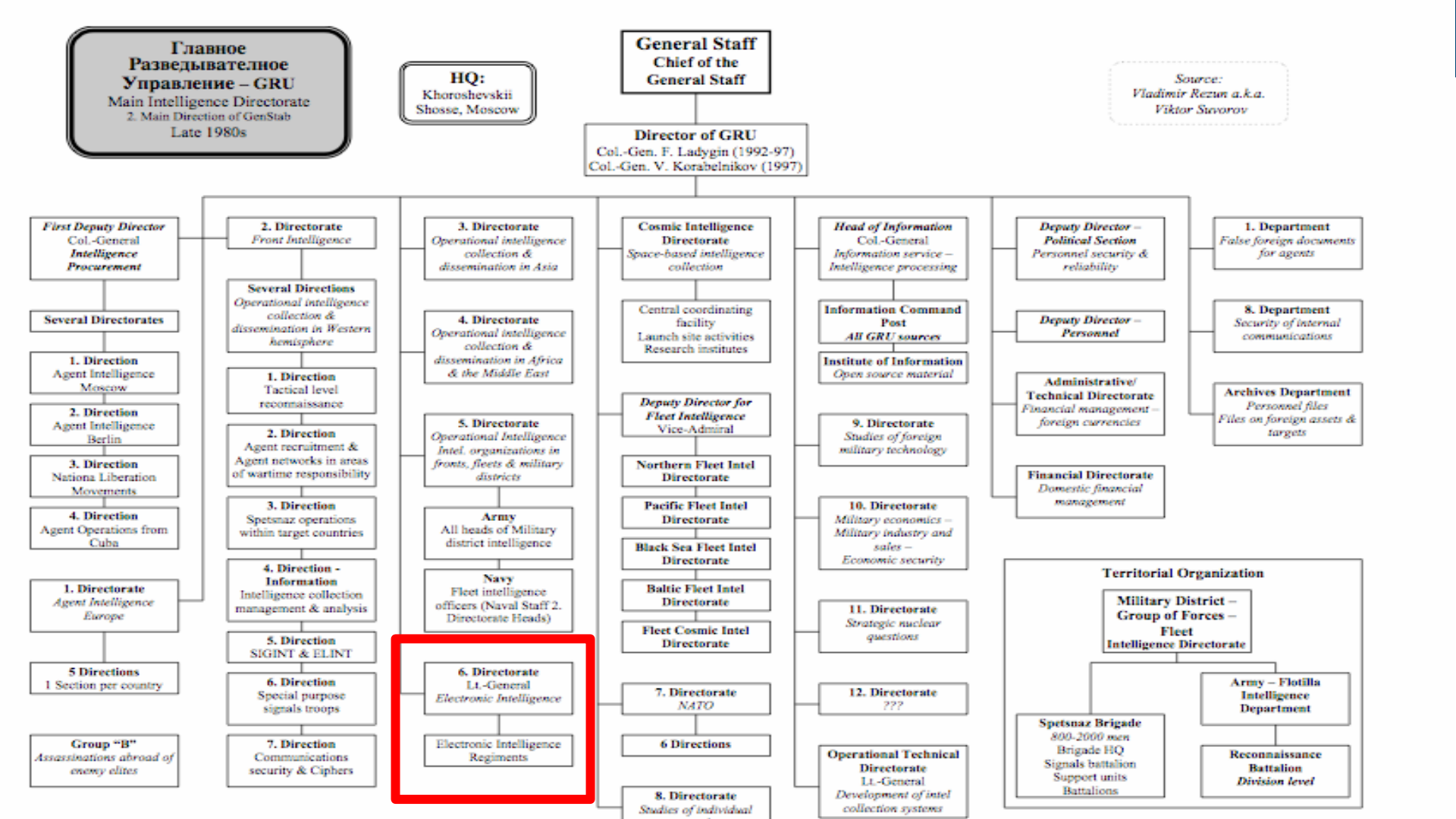
Disclaimer

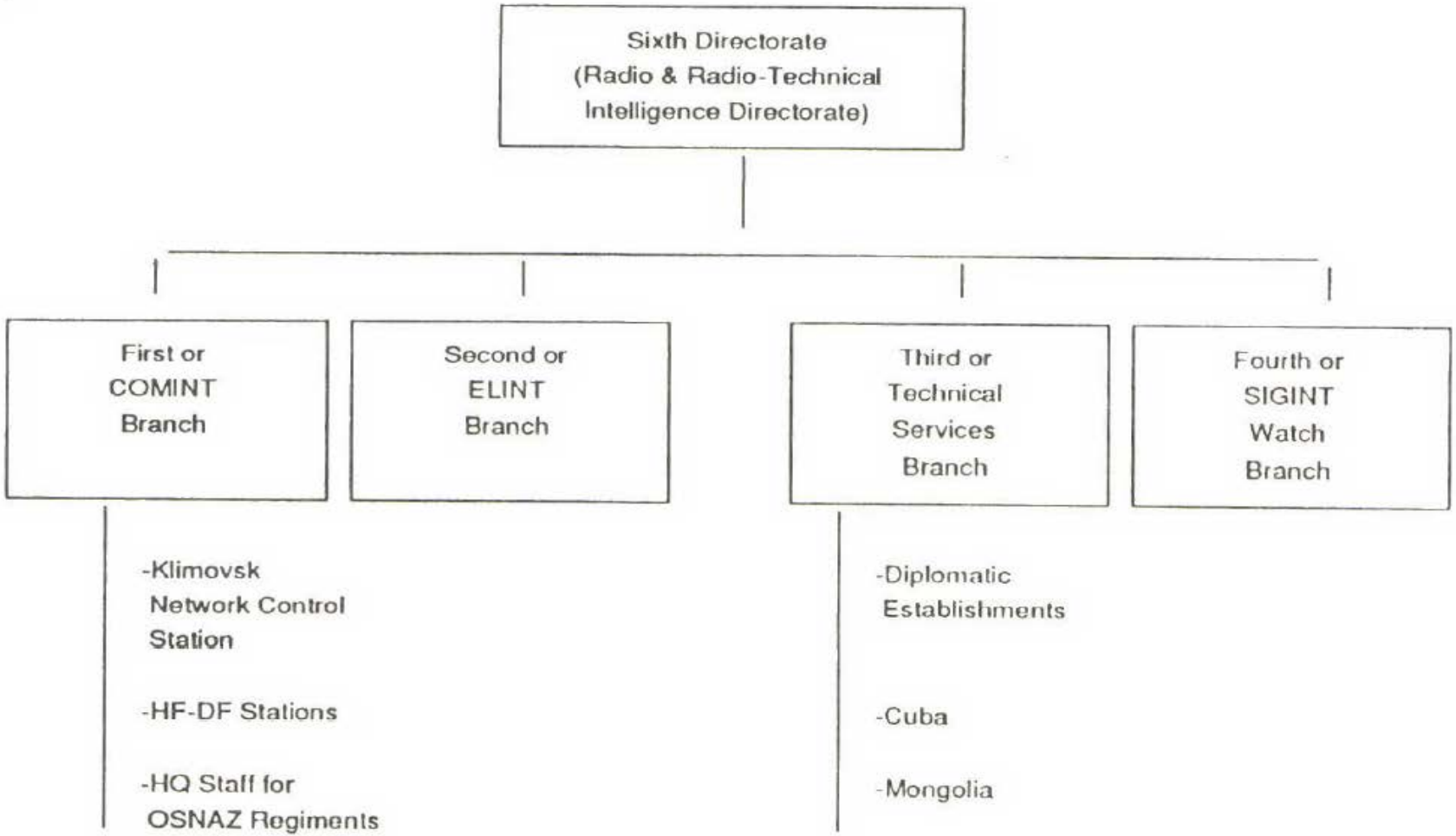
GRU: *Glavnoye Razvedyvatelnoye Upravlenie*

Vicealmirante Igor KOSTYUKOV (en funciones, 22/11)

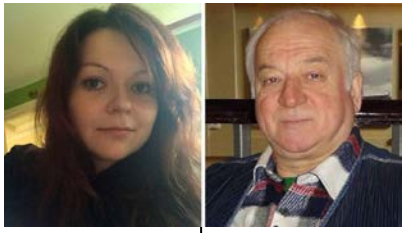
VCh 44388

- Necesidades de información
  - Militar
  - Política
  - Tecnología
  - Economía
  - Ecología
- Capacidades
  - SIGINT
  - HUMINT
  - OSINT
  - GEOINT
  - MASINT
  - TECHINT
  - …


Главное Разведывательное Управление – GRU
Main Intelligence Directorate
2. Main Direction of GenStab
Late 1980s
HQ:
Khoroshevskii Shosse, Moscow
General Staff
Chief of the General Staff
Source:
Vladimir Rezun a.k.a. Viktor Suvorov
Director of GRU
Col.-Gen. F. Ladygin (1992-97)
Col.-Gen. V. Korabelnikov (1997)
First Deputy Director
Col.-General
Intelligence Procurement
Several Directorates
1. Direction
Agent Intelligence Moscow
2. Direction
Agent Intelligence Berlin
3. Direction
Nationa Liberation Movements
4. Direction
Agent Operations from Cuba
1. Directorate
Agent Intelligence Europe
5 Directions
1 Section per country
Group "B"
Assassinations abroad of enemy elites
2. Directorate
Front Intelligence
Several Directions
Operational intelligence collection & dissemination in Western hemisphere
1. Direction
Tactical level reconnaissance
2. Direction
Agent recruitment & Agent networks in areas of wartime responsibility
3. Direction
Spetsnaz operations within target countries
4. Direction - Information
Intelligence collection management & analysis
5. Direction
SIGINT & ELINT
6. Direction
Special purpose signals troops
7. Direction
Communications security & Ciphers
3. Directorate
Operational intelligence collection & dissemination in Asia
4. Directorate
Operational intelligence collection & dissemination in Africa & the Middle East
5. Directorate
Operational Intelligence Intel. organizations in fronts, fleets & military districts
Army
All heads of Military district intelligence
Navy
Fleet intelligence officers (Naval Staff 2. Directorate Heads)
6. Directorate
Lt.-General
Electronic Intelligence
Electronic Intelligence Regiments
Cosmic Intelligence Directorate
Space-based intelligence collection
Central coordinating facility
Launch site activities
Research institutes
Deputy Director for Fleet Intelligence
Vice-Admiral
Northern Fleet Intel Directorate
Pacific Fleet Intel Directorate
Black Sea Fleet Intel Directorate
Baltic Fleet Intel Directorate
Fleet Cosmic Intel Directorate
7. Directorate
NATO
6 Directions
8. Directorate
Studies of individual
Head of Information
Col.-General
Information service – Intelligence processing
Information Command Post
All GRU sources
Institute of Information
Open source material
9. Directorate
Studies of foreign military technology
10. Directorate
Military economics – Military industry and sales – Economic security
11. Directorate
Strategic nuclear questions
12. Directorate
???
Operational Technical Directorate
Lt.-General
Development of intel collection systems
Deputy Director – Political Section
Personnel security & reliability
Deputy Director – Personnel
Administrative/ Technical Directorate
Financial management – foreign currencies
Financial Directorate
Domestic financial management
1. Department
False foreign documents for agents
8. Department
Security of internal communications
Archives Department
Personnel files
Files on foreign assets & targets
Territorial Organization
Military District – Group of Forces – Fleet
Intelligence Directorate
Army – Flotilla Intelligence Department
Spetsnaz Brigade
800-2000 men
Brigade HQ
Signals battalion
Support units
Battalions
Reconnaissance Battalion
Division level


Sixth Directorate
(Radio & Radio-Technical
Intelligence Directorate)
First or
COMINT
Branch
Second or
ELINT
Branch
Third or
Technical
Services
Branch
Fourth or
SIGINT
Watch
Branch
-Klimovsk
Network Control
Station
-HF-DF Stations
-HQ Staff for
OSNAZ Regiments
-Diplomatic
Establishments
-Cuba
-Mongolia

2018



03 marzo

13 julio

05 septiembre

National Cyber Security Centre
a part of GCHQ

Global Affairs Canada
Affaires mondiales Canada

04 octubre

21 noviembre

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)
VIKTOR BORISOVICH NETYKSHO,	*	
BORIS ALEKSEYEVICH ANTONOV,	*	
DMITRIY SERGEYEVICH BADIN,	*	
IVAN SERGEYEVICH YERMAKOV,	*	
ALEKSEY VIKTOROVICH LUKASHEV,	*	
SERGEY ALEKSANDROVICH MORGACHEV,	*	
NIKOLAY YURYEVICH KOZACHEK,	*	
PAVEL VYACHESLAVOVICH YERSHOV,	*	
ARTEM ANDREYEVICH MALYSHEV,	*	
ALEKSANDR VLADIMIROVICH OSADCHUK,	*	
ALEKSEY ALEKSANDROVICH POTEMKIN, and	*	
ANATOLIY SERGEYEVICH KOVALEV,	*	
	*	
Defendants.	*	
	*	

****

INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

WANTED BY THE FBI

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

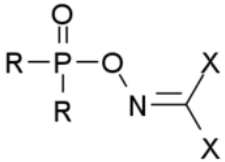

Aleksey Aleksandrovich Potemkin


Ivan Sergeyevich Yermakov


Pavel Vyacheslavovich Yershov

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

05/09/2018



GOV.UK

Alexander Petrov

Ruslan Boshirov

RT

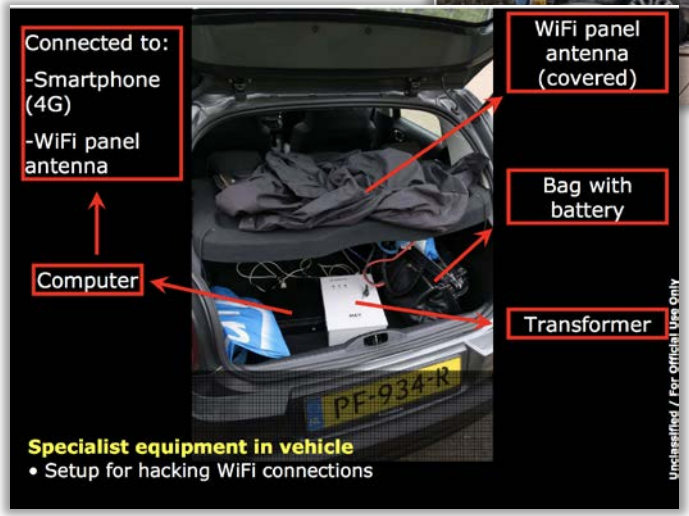
¿

Col. Anatoliy Chepiga
GRU Spetsnaz
Hero of the Russian Federation

Dr. Alexander Yevgeniyevich Mishkin
GRU Col/TCol
Hero of the Russian Federation

04/10/2018


Ministry of Defence
GRU close access cyber operation against OPCW
Genmaj. O. Eichelsheim
Defence Intelligence & Security Service
4 October 2018


Connected to:
-Smartphone (4G)
-WiFi panel antenna
Computer
WiFi panel antenna (covered)
Bag with battery
Transformer
PF-934-R
Specialist equipment in vehicle
• Setup for hacking WiFi connections
Unclassified / For Official Use Only


Unclassified / For Official Use Only
sday 10 April 2018
• Accompanied by embassy personnel
Unclassified / For Official Use Only


ALEKSEI
31.07.1979
ДИПЛОМАТИЧЕСКИЙ ПАСПОРТ
DIPLOMATIC PASSPORT

CIBER_ SEGURIDAD

National Cyber Security Centre
a part of GCHQ

04/10/2018

Attack	NCSC Assessment
In October 2017, BadRabbit ransomware encrypted hard drives and rendered IT inoperable. This caused disruption including to the Kyiv metro, Odessa airport, Russia's central bank and two Russian media outlets.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In August 2016, confidential medical files relating to a number of international athletes were released. WADA stated publicly that this data came from a hack of its Anti-Doping Administration and Management system.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In 2016, the Democratic National Committee (DNC) was hacked and documents were subsequently published online.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
Between July and August 2015 multiple email accounts belonging to a small UK-based TV station were accessed and content stolen.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.

Attack	
In June 2017 a destructive cyber attack targeted the Ukrainian financial, energy and government sectors but spread further affecting other European and Russian businesses.	GRU in February 2018. NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In October 2017, VPNFILTER malware infected thousands of home and small business routers and network devices worldwide. The infection potentially allowed attackers to control infected devices, render them inoperable and intercept or block network traffic.	In April 2018, the NCSC, FBI and Department for Homeland Security issued a joint Technical Alert about this activity by Russian state-sponsored actors.

#AlbornadasCENCERT

cni-cert
centro criptológico nacional

	NCSC Assessment
2018 GRU hackers sent spearphishing emails npersonated Swiss federal authorities to directly PCW employees, and thus OPCW computer . These employees were likely attending a ning conference in Spiez.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
2018 the GRU attempted to use its cyber ties to gain access to official OPCW computer networks.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to the UK Defence and Science Technology Laboratory (DSTL) computer systems.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In March 2018 the GRU attempted to compromise the UK Foreign and Commonwealth Office (FCO) computer systems via a spearphishing attack.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.

04/10/2018

FOR IMMEDIATE RELEASE Thursday, October 4, 2018

U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations

Conspirators Included a Russian Intelligence "Close Access" Hacking Team that Traveled Abroad to Compromise Computer Networks Used by Anti-Doping and Sporting Officials and Organizations Investigating Russia's Use of Chemical Weapons

A grand jury in the Western District of Pennsylvania has indicted seven defendants, all officers in the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces of the Russian Federation, for computer hacking, wire fraud, aggravated identity theft, and money laundering.

According to the indictment, beginning in or around December 2014 and continuing until at least May 2018, the conspiracy conducted persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government.

Global Affairs Canada
Affaires mondiales Canada

04/10/2018

Français

Government of Canada | Gouvernement du Canada

Search Canada.ca

Jobs | Immigration | Travel | Business | Benefits | Health | Taxes | More services

Home

Canada identifies malicious cyber-activity by Russia

From: Global Affairs Canada

Statement

October 4, 2018 – Ottawa, Ontario - Global Affairs Canada

Global Affairs Canada today issued the following statement:

"Today, Canada joins its allies in identifying and exposing a series of malicious cyber-operations by the Russian military. These acts form part of a broader pattern of activities by the Russian government that lie well outside the bounds of appropriate behaviour, demonstrate a disregard for international law and undermine the rules-based international order. Canada calls on all those who value this order to come together in its defence.

- **Unidades**
  - Identificación
  - Estructura
  - Funciones
  - Ubicación física
  - Personas
    - Identidades
      - Ámbito personal
      - Relaciones
    - Empleos
    - Funciones
    - Aliases
- **Operaciones**
  - OPSEC
    - Objetivos
    - TTP
    - Software
    - Artefactos
    - IOC

Unidad 74455

- Poca información pública.
  - Publicaciones científicas sobre *jamming*, criptografía…
- Ubicación: Kirova, 22 (Khimki, Moscú).
- Cometido: manejo de información. PSYOP.
  - *Dezinformatsiya, spetspropaganda, informatsionnoye protivoborstvo, kompromat*…
  - Sockpuppets: DCLeaks, Guccifer 2.0.
  - Mantenimiento de infraestructura.

Unidad 74455

Aleksandr
VLADIMIROVICH OSADCHUK

Anatoliy
SERGEYEVICH KOVALEV

Aleksey
ALEKSANDROVICH POTEMKIN

УДОСТОВЕРЕНИЕ

НА РАЦИОНАЛИЗАТОРСКОЕ ПРЕДЛОЖЕНИЕ

№ 247

В соответствии с пунктом 8 «Положения об открытиях, изобретениях и рационализаторских предложениях» настоящее удостоверение выдано подполковнику ЗАБЕЛИНУ Евгению Максимовичу (фамилия, имя, отчество) капитану МЕЛЬНИКОВУ А.Ф.

на принятое в войсковой части 26165 (наименование части, учреждения, организации) к внедрению рационализаторское предложение "Программа получения разностей по заданным параметрам (№ -123с)". (наименование предложения)

КОМАНДИР ВОЙСКОВОЙ ЧАСТИ 26165
(м. п.) ГЕНЕРАЛ-МАЙОР (ОЛУСОВ)

31 января 1970 г.

Unidad 26165

- Servicio de descifrado del GRU (histórico), activo desde el **23/05/1953**.
  - Dependencia directa de la Dirección del GRU.
- Ubicación: Komsomolsky prospekt, 20 (Moscú).
  - Junto a Unidad Militar 06410 (*152nd Special Training Center*).
- Cometido: Compromiso técnico de objetivos. CNO.
  - Actividades hostiles.
  - Desarrollo de capacidades técnicas.
  - Mantenimiento y operación de infraestructura.

Unidad 26165

Viktor
BORISOVICH
NETYKSHO

Boris
ALEKSEYEVICH
ANTONOV

Sergey
ALEKSANDROVICH
MORGACHEV

Dmitriy
SERGEYEVICH
BADIN

Ivan
SERGEYEVICH
YERMAKOV

Aleksey
VIKTOROVICH
LUKASHEV

Nikolay
YURYEVICH
KOZACHEK

Pavel
VYACHESLAVOVICH
YERSHOV

Artem
ANDREYEVICH
MALYSHEV

Unidad 26165

Aleksei SERGEYEVICH MORENETS

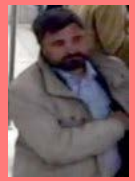
Evgenii MIKHAYLOVICH SEREBRIAKOV

Dmitriy SERGEYEVICH BADIN

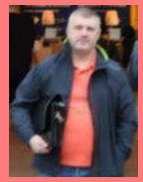
Artem ANDREYEVICH MALYSHEV

Ivan SERGEYEVICH YERMAKOV

¿Unidad 22177?



Alexey VALEREVICH MININ



Oleg MIKHAYLOVICH SOTNIKOV

Otras unidades GRU

- **VCh 11135.**
  - Diseño equipamiento SIGINT, dispositivos inalámbricos, seguridad SCADA, protección comunicaciones.
- **VCh 40904.**
  - Procesamiento SIGINT.
- **VCh 36360.**
  - Formación avanzada en inteligencia, incluyendo ciber.
- **VCh 54726.**
  - Análisis de capacidades de países extranjeros, incluyendo ciber.
- …

Otras unidades MOD

- **VCh 31659.**
  - Protección lógica MOD.
- **VCh 01168.**
  - Potencia de cálculo. Desinformación.
- **VCh 96010.**
  - Control tecnologías “sensibles”. Exportación.
- **VCh 21882, 77111, 33872.**
  - Guerra electrónica.
- **VCh 40056.**
  - Dirección Principal de Investigación Submarina.
- …

Objetivos

Objetivo/Campaña	US	UK	CA	NL
USA 2016				
Democratic Congressional Campaign Committee (DNCC)	X			
Democratic National Committee (DNC)	X	X		
Novichok				
Organisation for the Prohibition of Chemical Weapons (OPCW)	X	X	X	X
Laboratorio/Conferencia Spiez (Berna, Suiza)	X	X		X
UK Defense and Science Technology Laboratory (DSTL)		X		
UK Foreign and Commonwealth Office (FCO)		X		

Objetivos

Objetivo/Campaña	US	UK	CA	NL
Dopaje				
World Anti-Doping Agency (WADA)	X	X	X	
Canadian Centre for Ethics in Sport (CCES)	X		X	
US Anti-Doping Agency (USADA)	X			
Juegos Olímpicos Rio de Janeiro 2016	X			X
Laboratorio/Congreso WADA Laussanne (Suiza)	X			X
International Association of Athletics Federations (IAAF)	X			
Fédération Internationale de Football Association (FIFA)	X			

Objetivos

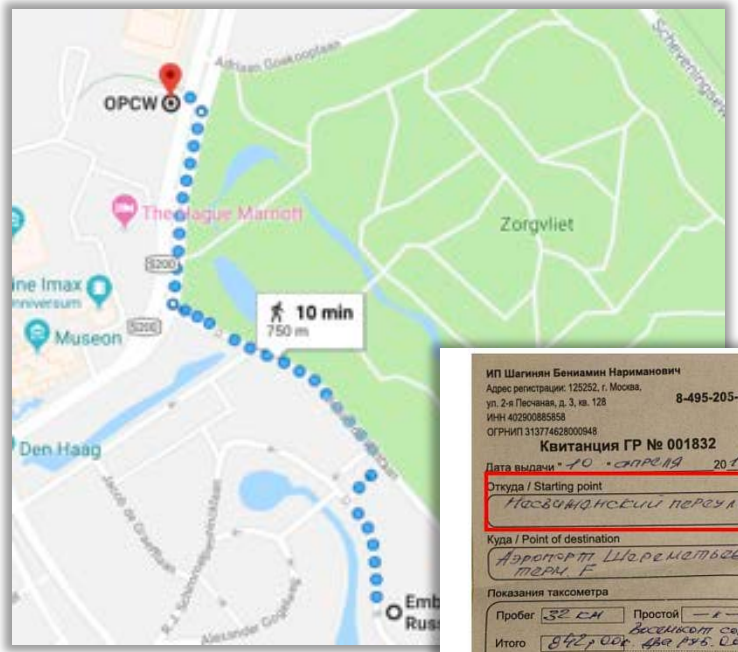
Objetivo/Campaña	US	UK	CA	NL
MH17				
Investigación holandesa				X
Hotel Kuala Lumpur (Malasia)				X
Ucrania				
NotPetya		X		
BadRabbit		X		

TTP

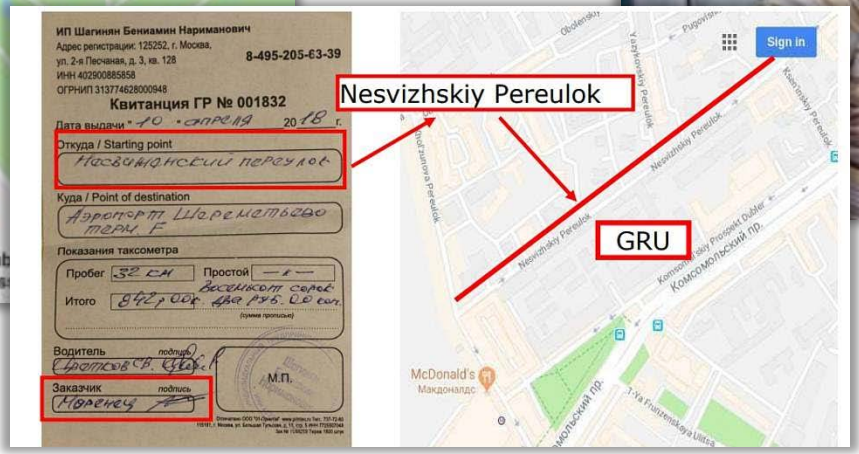
TÁCTICA	TÉCNICA
Reconocimiento	OSINT
Reconocimiento	Reconocimiento activo
Intrusión	Relaciones de confianza: explotación de terceros para llegar al objetivo final
Intrusión	Uso de credenciales válidas, obtenidas en algunos casos gracias a los ataques de spearphishing
Intrusión	Spearphishing mediante enlaces dañinos en correos electrónicos, con acortadores de URL
Intrusión	Spearphishing mediante anexos dañinos (MS Office)
Intrusión	Close Access
Ejecución	Explotación de vulnerabilidades en el cliente
C2	Uso de proxies para dificultar la traza de comunicaciones
Descubrimiento	Rastreo y búsqueda de archivos y directorios
Adquisición	Recolección automática de información, tanto técnica -de la infraestructura de la víctima- como de interés de inteligencia mediante herramientas públicas
Adquisición	Captura de datos introducidos por el usuario, por ejemplo vía keylogging
Adquisición	Captura de correos electrónicos directamente de servidores Microsoft Exchange
Adquisición	Adquisición de archivos de endpoints, vía forfiles
Adquisición	Capturas de pantalla en las víctimas
Exfiltración	Compresión de datos previa a la exfiltración, mediante herramientas públicas
Evasión	Borrado de archivos para evitar detección o extracción de inteligencia técnica, con CCleaner
Evasión	Borrado de registros en sistemas comprometidos, para evitar detección o extracción de inteligencia técnica, mediante wevtutil (wevtutil cl System y wevtutil cl Security)
Persistencia	Robo de credenciales mediante herramientas públicas y desarrollos propios
Destrucción	Cifrado y borrado de objetos

OPSEC

Cobertura

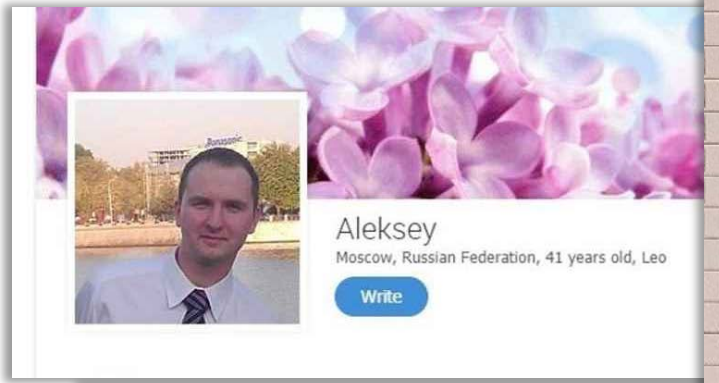


Compartimentación



Ocultación

OPSEC



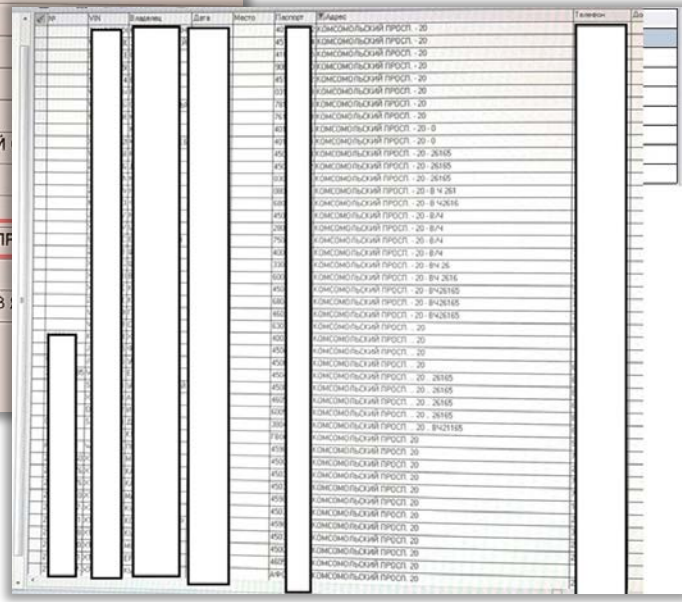
Serebryakov Evgeny Mikhai

Edad: 37

Fecha de nacimiento: 07.27.1981

Clubes de jugadores: agente libre (zach. , LFL,

Название поля	Значение
Системный номер	5899138
Дата	070404
Тип операции	Регистрация снятых с учета (из комм. магазина)
Госномер	О509ОА97
Марка	ВАЗ 21093
Цвет	СЕРЫЙ/МЕТАЛЛИК
Год выпуска	00
Мощность л.с.	68
ПТС	63ЕС769740
№ кузова	ХТА210930Y2737711
№ шасси	ХТА210930Y2737711
№ двигателя	210832856007
VIN	ХТА210930Y2737711
Владелец	МОРЕНЕЦ АЛЕКСЕЙ
Дата рождения	31.07.1977
Паспорт	450
Адрес	КОМСОМОЛЬСКИЙ ПР
Телефон	2190518
Тип базы	Гибдд по Москве от 23



OPSEC

¡Esto pasa hasta en las mejores familias!

Preguntas y conspiraciones

01
¿Cómo se ha obtenido esta información?

02
¿Por qué se publica tanto nivel de detalle?

03
¿Por qué sólo el GRU?

04
¿Es APT28 el GRU?
¿La Unidad 26165?
¿La Unidad 74455?
¿Ambas?

05
Después de lo que ha pasado…
¿el GRU ya no es tan bueno?
¿seguirá operando en ciber?

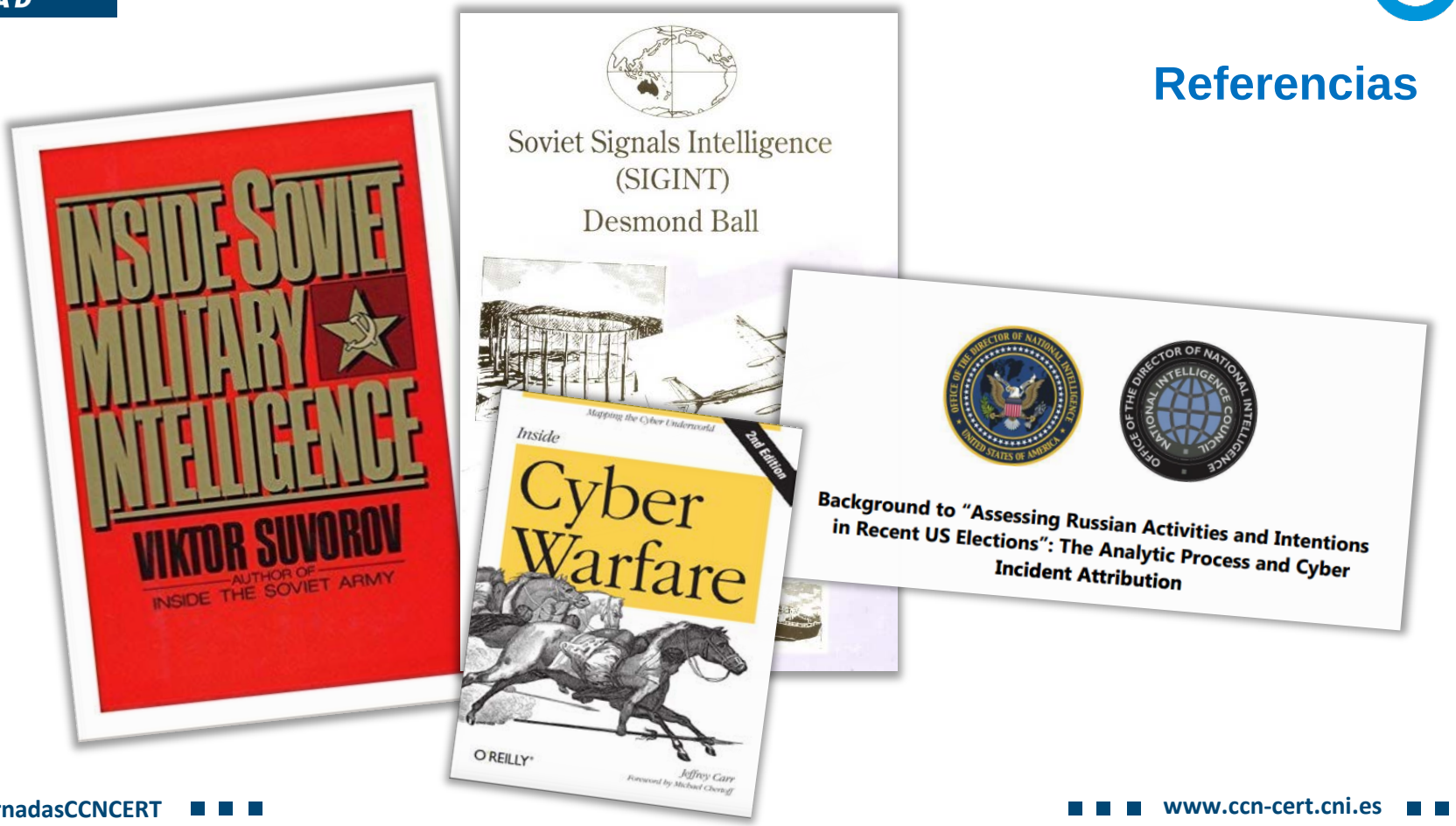
Conclusiones

- Duro golpe al GRU en 2018, pero…
  - GRU como actor muy relevante en el ámbito ciber (y no ciber).
  - Rusia como actor muy relevante en el ámbito ciber (y no ciber).

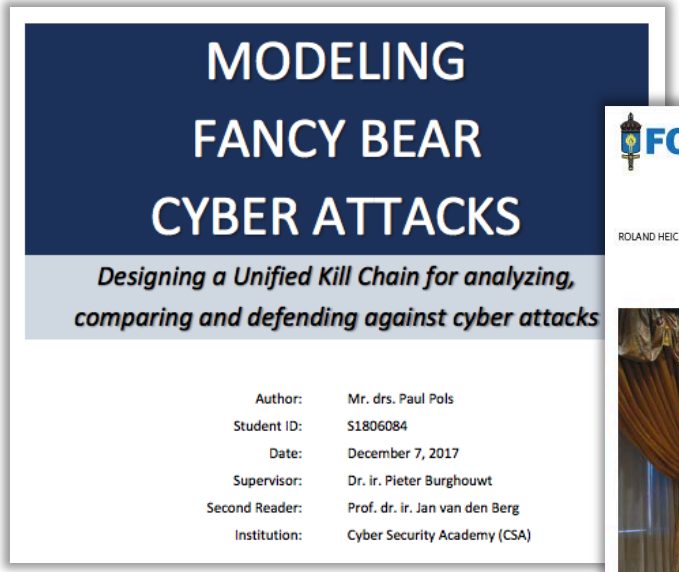
- *Information confrontation (IPb, informatsionnoye protivoborstvo)*.
  - Informativo-Técnico: CNO. VCh 26165.
  - Informativo-Psicológico. PSYOP. VCh 74455.

- APT28: ~~*fancy*~~ *old bear.*

Referencias

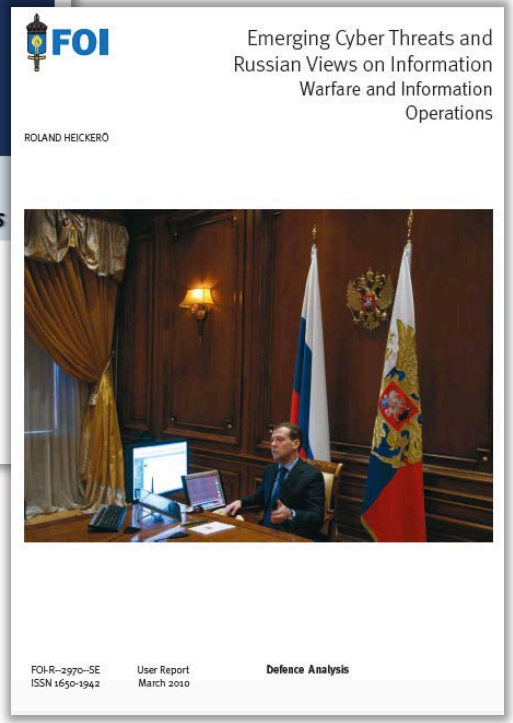


Referencias


MODELING
FANCY BEAR
CYBER ATTACKS

Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks

Author: Mr. drs. Paul Pols
Student ID: S1806084
Date: December 7, 2017
Supervisor: Dr. ir. Pieter Burghouwt
Second Reader: Prof. dr. ir. Jan van den Berg
Institution: Cyber Security Academy (CSA)


FOI

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations

ROLAND HEICKERÖ

FOI-R--2970--SE
ISSN 1650-1942

User Report
March 2010

Defence Analysis

Global Affairs Canada
Affaires mondiales Canada

National Cyber Security Centre
a part of GCHQ

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

CCN-CERT centro criptológico nacional