VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

RỦI RO ATTT TRONG NGUY CƠ XUNG ĐỘT KỸ THUẬT SỐ TOÀN CẦU

TS. VÕ VĂN KHANG

XUNG ĐỘT KỸ THUẬT SỐ TOÀN CẦU LÀ GÌ ?

Sử dụng các công cụ kỹ thuật số để giải quyết tranh chấp hoặc thực hiện tấn công đối thủ trên môi trường mạng!

1 XUNG ĐỘT DIỆN RỘNG – WORLD WAR

2 XUNG ĐỘT KHU VỰC RẤT GẦN VỚI VIỆT NAM

3 XUNG ĐỘT KHI VIỆT NAM LÀ MỘT BÊN LIÊN QUAN

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

1. Russia – Ukraine Cyberwar Case Study

2. Rủi ro ATTT cho Việt Nam

3. Một số đề xuất, kiến nghị

1. Russia – Ukraine Case Study

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

VietnamNet
VÌ VIỆT NAM HÙNG CƯỜNG

COVID-19 | Công nghệ số và truyền thông | Tin nóng

Chính trị | Thời sự | Kinh doanh | Thế giới | Giải trí | Thể thao | Sức khỏe | Đời sống | Giáo dục | Pháp luật | Xe | Công nghệ

CÔNG NGHỆ > BẢO MẬT

Nga thử nghiệm đối phó với tình hu
phương cô lập khỏi internet toàn cầ

189 | Zalo | Theo dõi VietNamNet trên Google News

**Mạng Runet nội địa của Nga khác với hệ thống "Đại Tường lửa" của Trung Quố
bị cho tình huống bị thế lực thù địch tấn công mạng và họ phải ngắt toàn bộ kết
internet toàn cầu.**

Kể từ năm 2019, các thành phố trên khắp nước Nga đã và đang thử nghiệm các cách thức
của hệ thống internet (thường được gọi là Runet) ra khỏi mạng kết nối toàn cầu rộng lớn hơn.

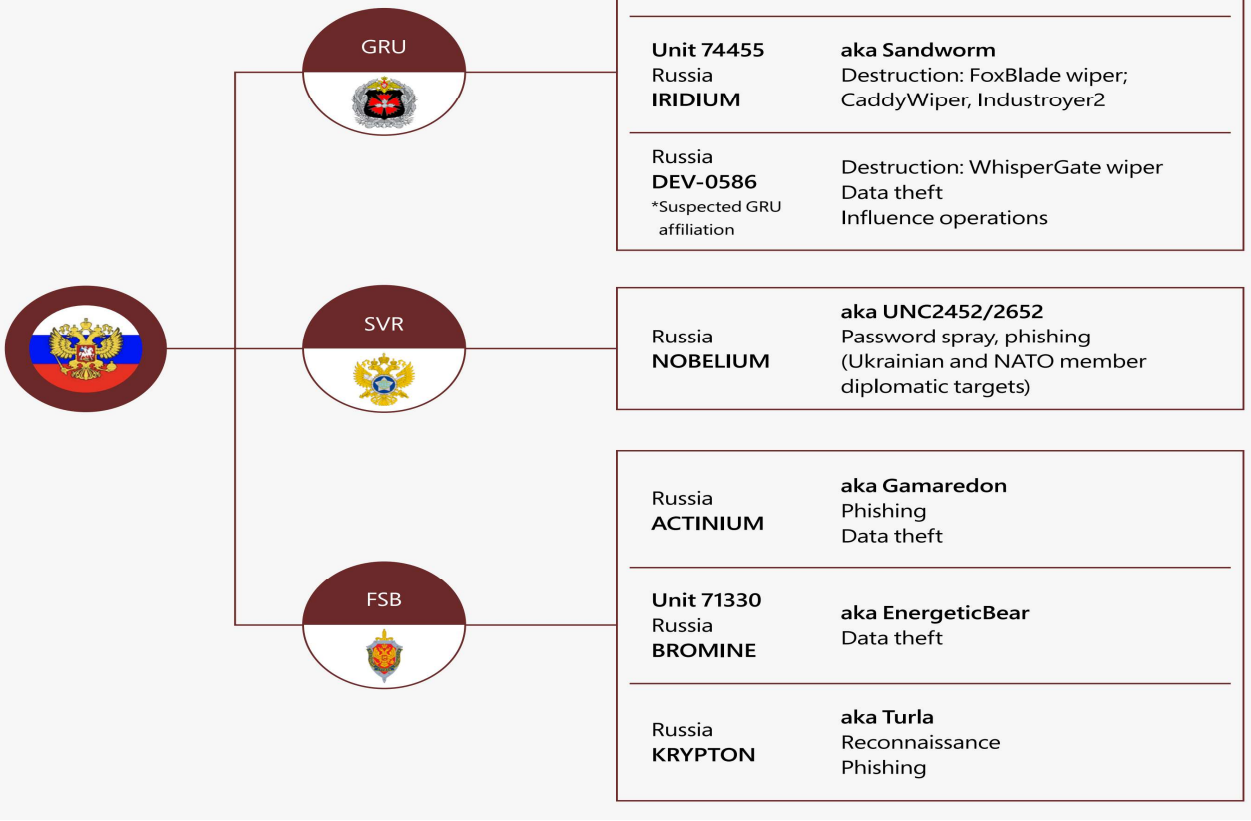
1. Russia – Ukraine Case Study

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

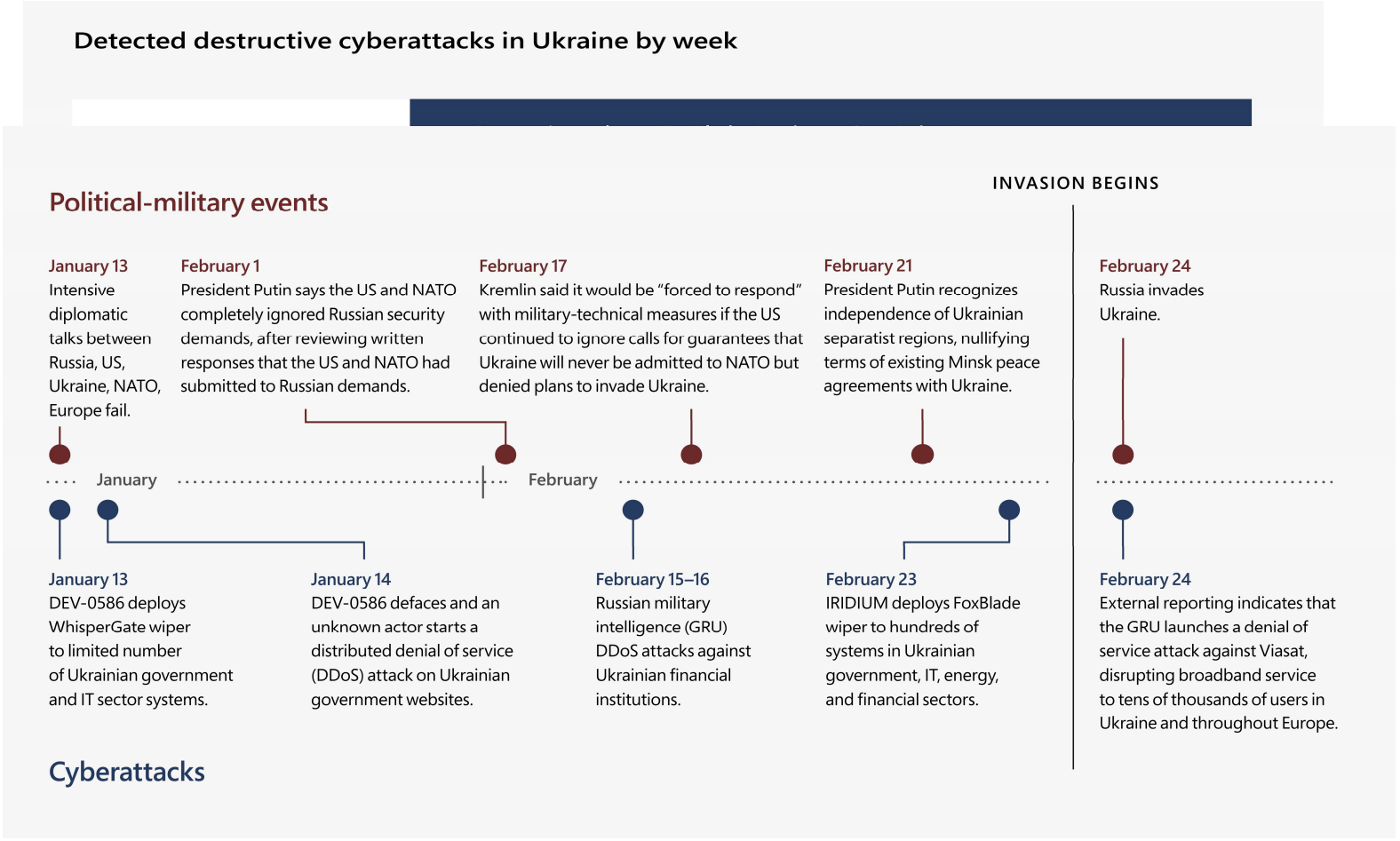
Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- **The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18**
- **Russian Foreign Intelligence Service (SVR)**
- **Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)**
- **GRU's Main Center for Special Technologies (GTsST)**
- **Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)**

1. Russia – Ukraine Case Study

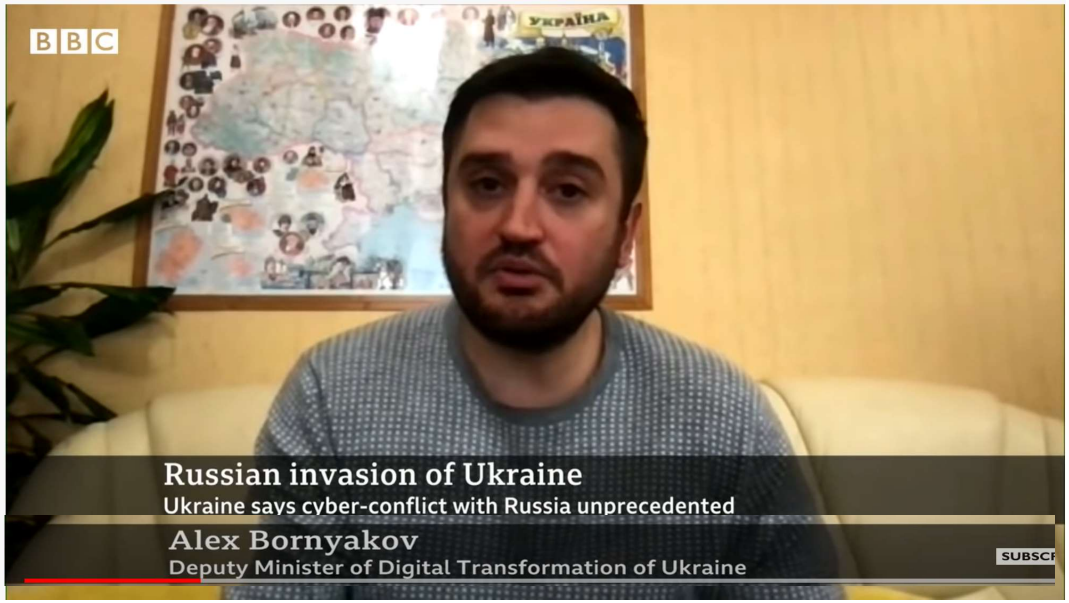


1. Russia – Ukraine Case Study



1. Russia – Ukraine Case Study

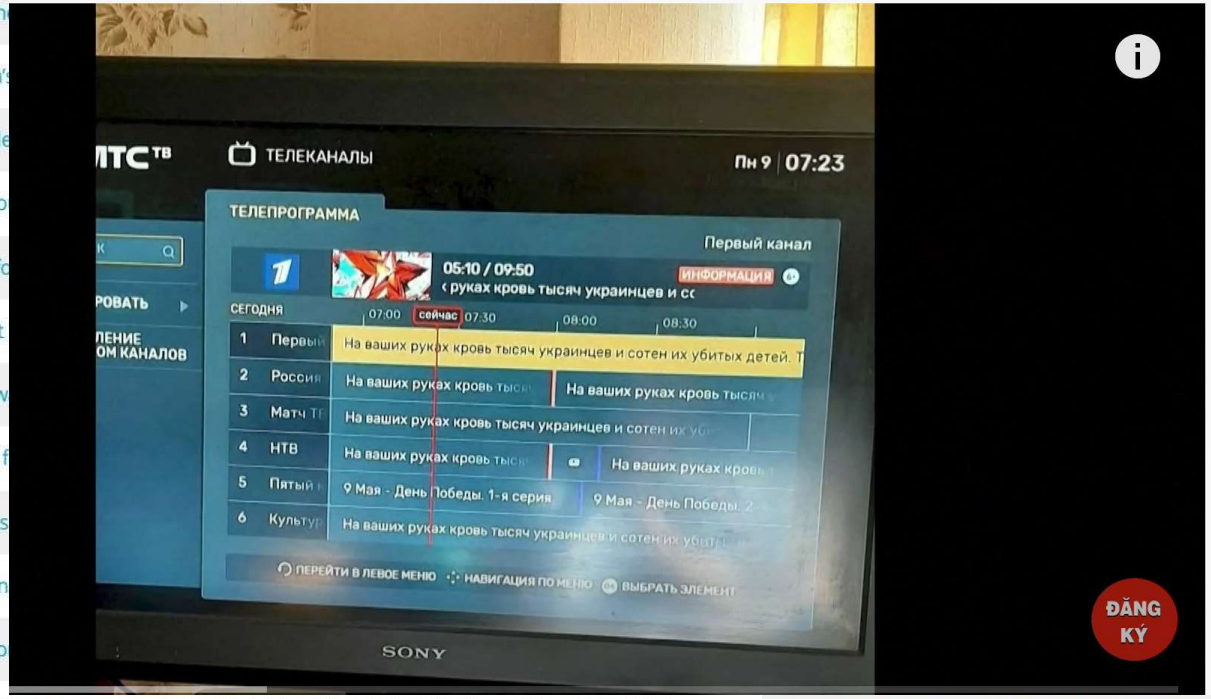
- 300k hackers tham gia cuộc chiến chống Nga (theo Netblock)
- Social Attacks - Ukraine vượt trội
- Starlink của Elon Musk hỗ trợ Ukraine kết nối Internet



1. Russia – Ukraine Case Study

Daily Report from Anomali ！

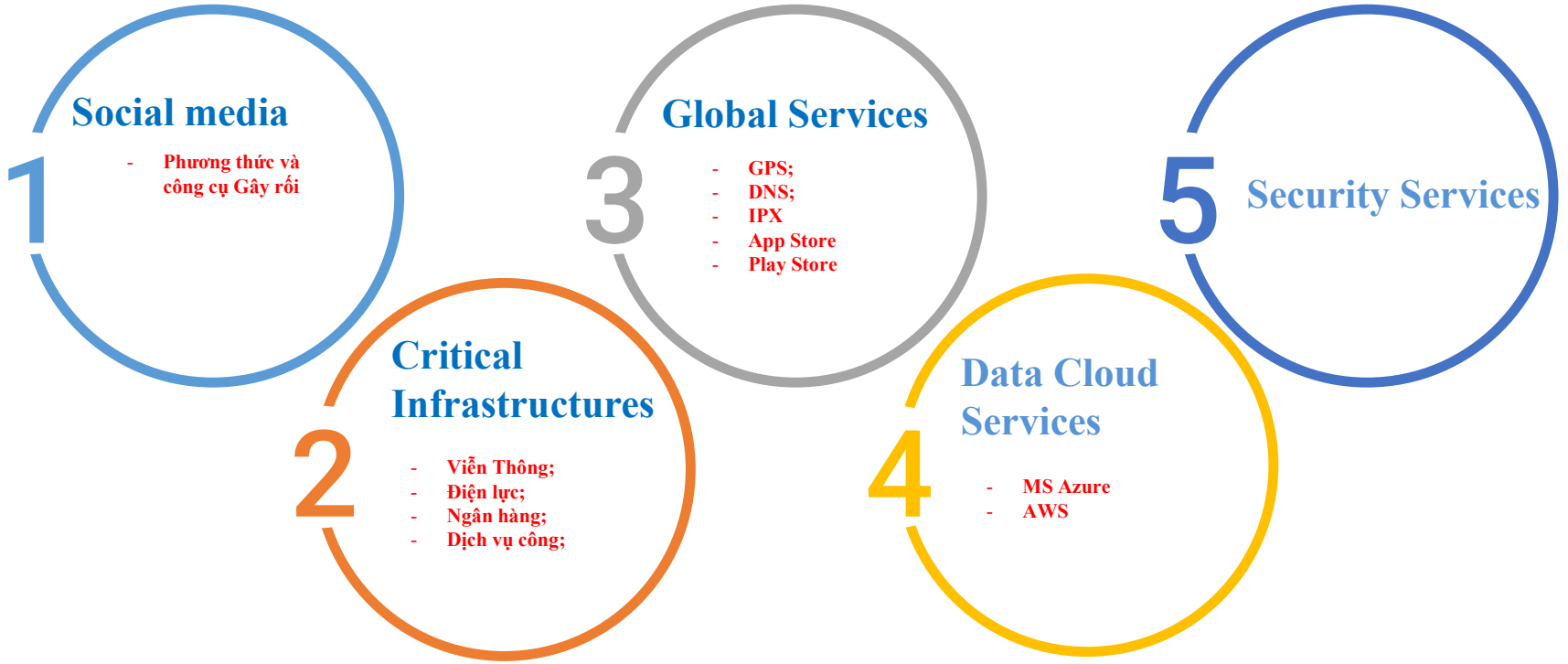
Security Affairs: Ukraine IT Army hit EGAIS portal impacting Russia's alcohol distribution	06 May 2022 18:00
CyberNews: Russian aviation authority switch	
CyberNews: Hackers breach Rosatom, Russia's	
CyberNews: Russian social media giant VK alle	
Security Affairs: Security Affairs newsletter Ro	
Security Boulevard: Stormous Claims Credit fo	
Bleeping Computer: Microsoft says Russia hit	
Bleeping Computer: US offers $10 million rew	
Security Week: US Offers $10 Million Reward f	
Graham Cluley: Ukraine's postal service prints	
CISA: AA22 110A Joint CSA Russian State Spon	
Security Affairs: Security Affairs newsletter Ro	
Bulletin for AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical...	22 Apr 2022 03:01
Partner Intel Product: RU Actors Threats to Crit. Infrastructure (Was: Joint Cybersecurity Advisory AA...	21 Apr 2022 12:09



Name	Modified
se in Card Fraud	09 May 2022 18:17
argeting embassies - SEKOIA.IO	09 May 2022 17:12
rity	09 May 2022 16:56
ecurity	09 May 2022 05:01
	09 May 2022 05:12
ict	09 May 2022 02:07
e campaña de phishing pro-rusas	08 May 2022 19:25
	07 May 2022 18:27
з використанням тематики хімічної ...	09 May 2022 16:55
ами CredoMap_v2 (CERT-UA#4622)	07 May 2022 18:25
(CERT-UA#4622)	09 May 2022 16:56
andiant boss	07 May 2022 18:15
	09 May 2022 16:57
ving invasion	07 May 2022 04:12
ssian entities	07 May 2022 00:48
ated on 2022-05-06 13:19:44	09 May 2022 16:58
Shuckworm Itensifies Ukraine Cyberwar | The Dock on the Bay | Threat Bulletin Created on 2022-05-06 13:11:...	06 May 2022 21:15
s2wblog: Rising Stealer in Q1 2022: BlackGuard Stealer | by S2W | S2W BLOG | Apr, 2022 | Medium	09 May 2022 17:04

2. RỦI RO ATTT CHO VIỆT NAM

Các khu vực dễ bị tổn thương !



2. RỦI RO ATTT CHO VIỆT NAM

1. XUNG ĐỘT DIỆN RỘNG – WORLD WAR
2. XUNG ĐỘT KHU VỰC RẤT GẦN VỚI VIỆT NAM
3. XUNG ĐỘT KHI VIỆT NAM LÀ MỘT BÊN LIÊN QUAN

3. MỘT SỐ KIẾN NGHỊ

1. **Có đơn vị chuyên trách để đánh giá rủi ro và xử lý trong tình huống xảy ra xung đột**
   Đánh giá một cách nghiêm túc về các ảnh hưởng trong 3 kịch bản xung đột có thể diễn ra để xây dựng giải pháp ứng phó

2. **Diễn tập về khả năng sinh tồn trong môi trường cô lập**
   Cần có kịch bản diễn tập trong tình huống mất kết nối Internet toàn cầu từng phần hoặc toàn bộ

3. **Nâng cao năng lực về ATTT – đặc biệt là xây dựng lực lượng**
   Cần có quy hoạch rõ ràng về việc nâng cao năng lực về hạ tầng, ứng dụng, tính toán hiệu năng cao, và đặc biệt là nhân sự về ATTT

4. **Hợp tác quốc tế thông qua Hiệp hội – Tham gia các liên minh chiến lược (Phi chính phủ)**
   Thực tế chứng minh không một quốc gia nào đơn độc có thể đứng vững trước tấn công hội đồng – cần có sự hỗ trợ từ cộng đồng quốc tế

VIETNAM INFORMATION SECURITY ASSOCIATION

website: www.vnisahcm.org.vn

BRANCH OFFICE
Lot E2a-3, D1 St., Saigon High-Tech Park (SHTP),
Long Thanh My Ward, Thu Duc City, HCMC, Vietnam
Tel: (84-28) 73 030 309

Thank You!