
# THE PROXY WARFARE:
# UNMASKING RUSSIAN AND CHINESE EXTERNALIZED CYBER CAPABILITIES

# WHO I AM?

**ALIXIA RUTAYISIRE**

- Geopolitical Analyst at QUOINTELLIGENCE
- Previous role as intelligence analyst at the French MoD
- Assessment of political and security situations
- Providing strategic insights combining geopolitics and CTI

# SETTING THE STAGE: Methodology, Scope, Structure

**Methodology**

- Leaks
- US Indictements
- Intelligence agencies' reports
- Academic research
- CTI companies' reports

→ Building on the notion of CAPITAL INTELLIGENCE

**Scope**

- Participation of non-state actors in cyber operations to the benefit of a State
- Focus on private companies
- Front companies are out of scope


**Structure**

- Russia's case
- China's case
- Comparative analysis
- Conclusions

# RUSSIA: Cybercrime network historical development

**Dissolution of the USSR (1991)**

**Security Vacuum**

- Weak law enforcement
- Deregulated environment

**Economic Collapse**

- Rapid privatization - Wild West economy
- Limited economic opportunities for highly educated IT engineer

**Crime Increase**

**Organized Crime**

Underpaid or unpaid Intelligence officers

**Cyber Crime**

Underpaid or unpaid Intelligence officers

# RUSSIA: Intelligence agencies behind warfare apparatus

Presidential Administration

FSB

**Domestic intelligence**

- Counterintelligence and law enforcement
- Scope includes Russia's near-abroad

SVR

**External civilian intelligence**

- Conducts strategic, economic, scientific and technological espionage

GRU

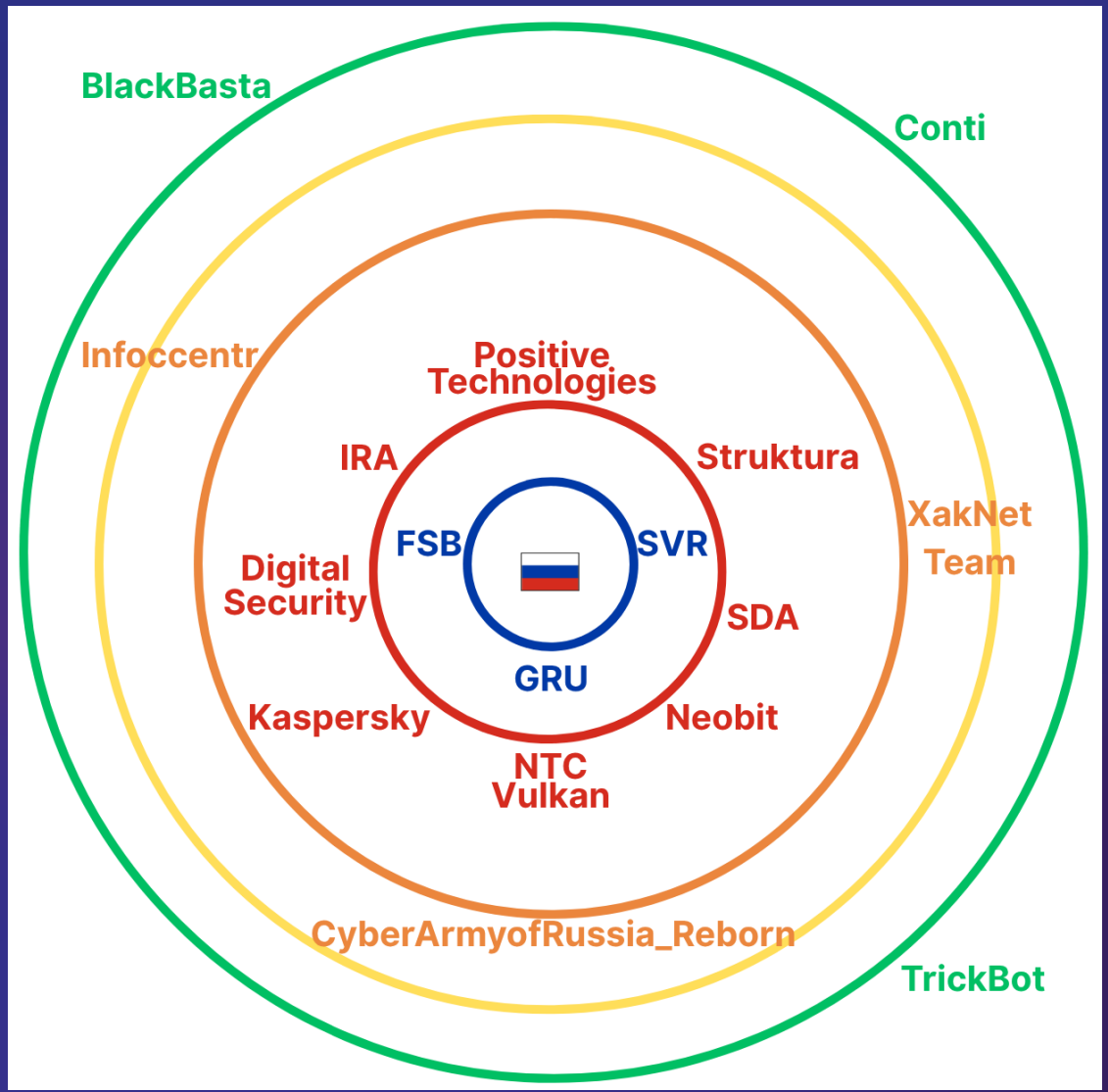
**Military intelligence**

- Broarder scope matching Russia's strategic interests

# RUSSIA:
# The outsourcing ecosystem

Layers of outsourcing:

- intelligence agencies
- private companies
- hacktivist groups
- lone wolves
- eCrime groups



# RUSSIA: Proxy services offering

Vulnerability Identification

Tools & Solutions

Recruiting

Training


Information Operation

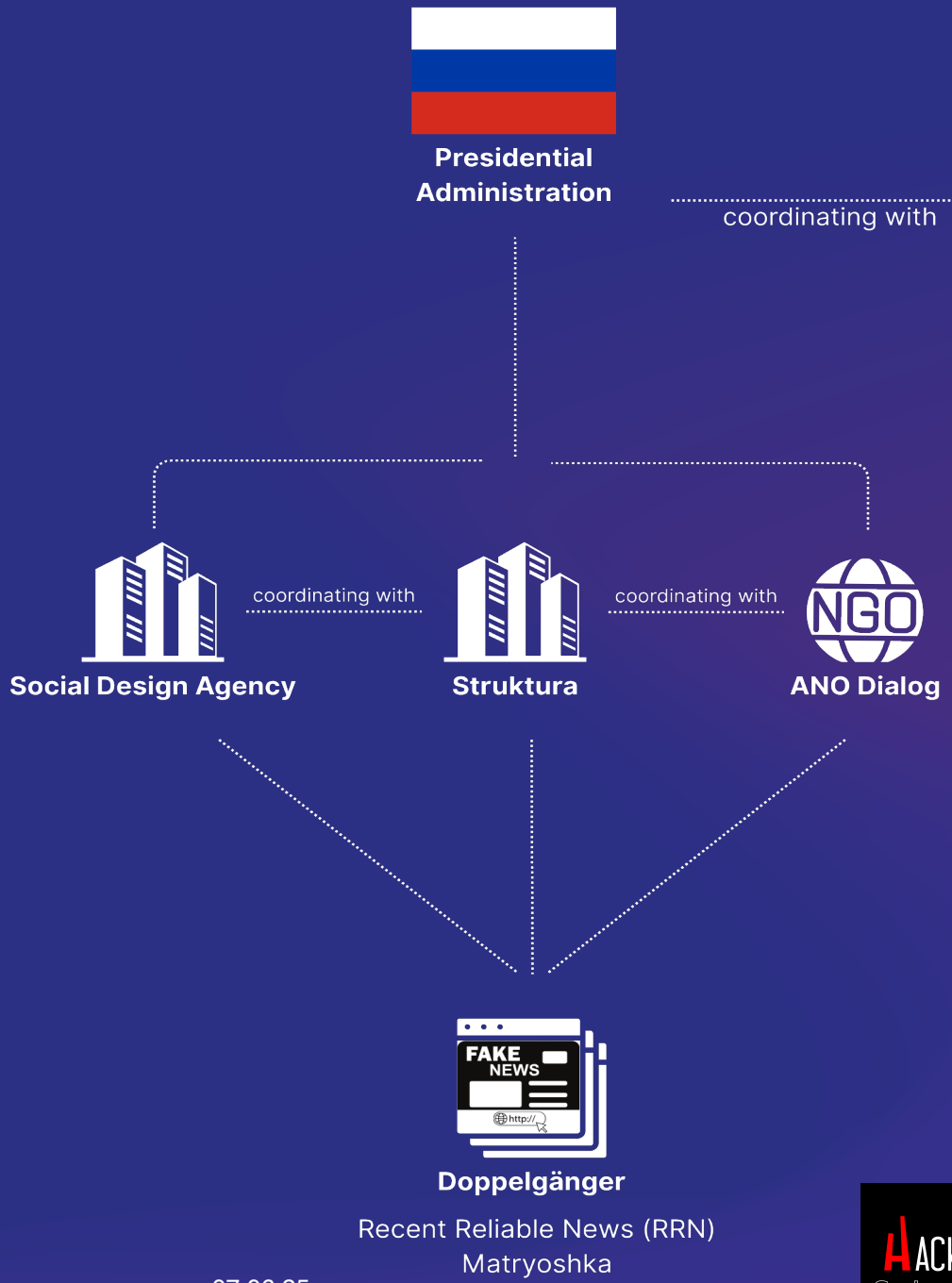
# RUSSIA: Outsourcing risk-benefit calculus

**RISKS**

- Lack of control
- Risky behavior
- Uncertain mobilization

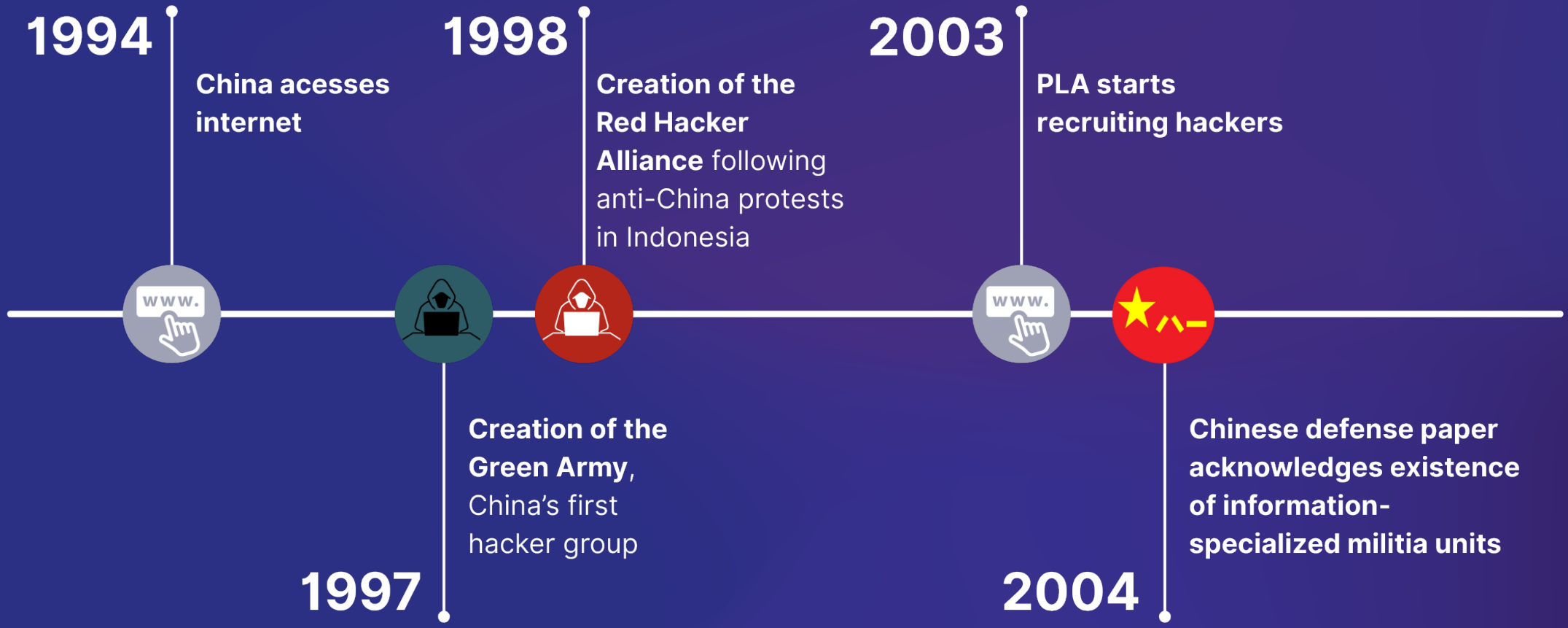
**BENEFITS**

- Reduced costs
- Flexibility
- ~~Plausible deniability~~




# RUSSIA: The IO network

# CHINA: Cyber sphere historical development



# CHINA: From patriotic hackers to state contractors

Wu Haibo

Member of the Green Army

I-Soon

Cai Jingjing

Member of the Red Hacker Alliance

Integrity Tech

Tan Dailin

Founder of NCPH Hacking Group

PLA

Arrested by the MPS

MSS

Founder of cybersecurity firms

# CHINA: Institutional architecture of state cyber capabilities

CCP Politburo

PLA

China military

- Cyber and psychological warfare

State Council

Ministry of Industry and Information Technology

MSS

Civilian intelligence and security service

- Counterintelligence
- Foreign intelligence
- Political security and domestic stability
- Strong provincial organs

MPS

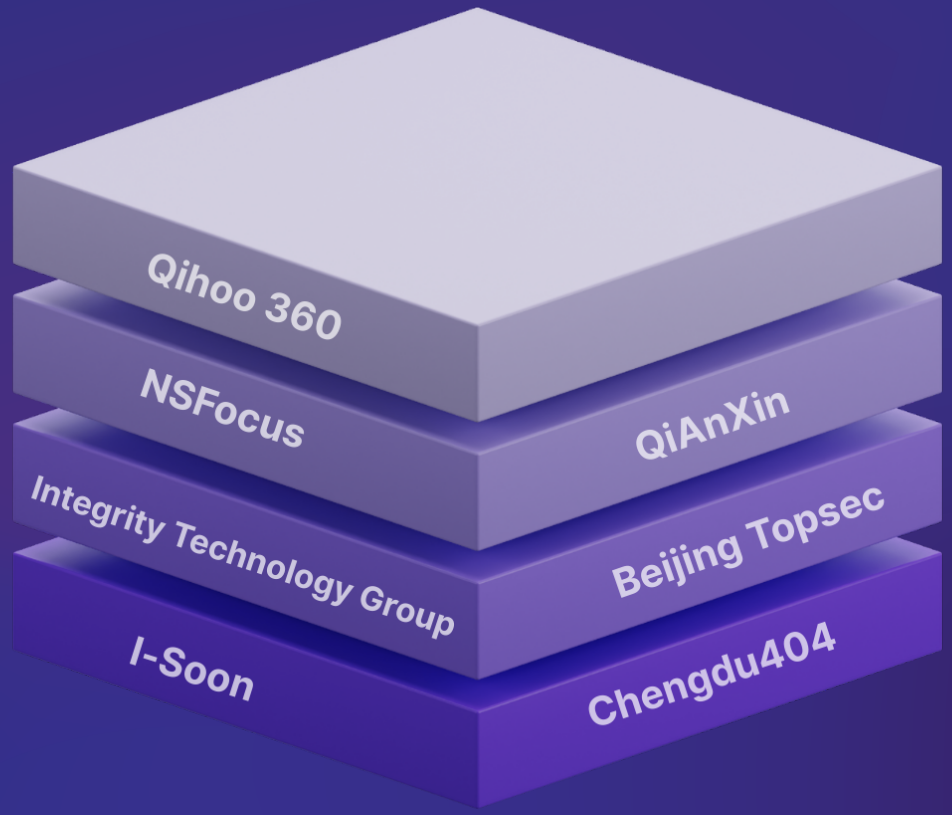
Law enforcement agency

- Police and homeland security

# CHINA: The outsourcing ecosystem

**Key Characteristics:**

- Comprehensive national strategy
- Public bids
- IT leaders and SMEs
- Subcontracting
- Competitive environment
- Links based *guanxi*
- High degree of autonomy



# CHINA: Proxy services offering

Vulnerability Identification

Hacking-for-hire

Tools & Solutions

Recruiting


Information Operation

# CHINA: Outsourcing risk-benefit calculus

**RISKS**

- Companies or employees re-selling data
- Corruption and bid rigging
- Risky behavior

**BENEFITS**

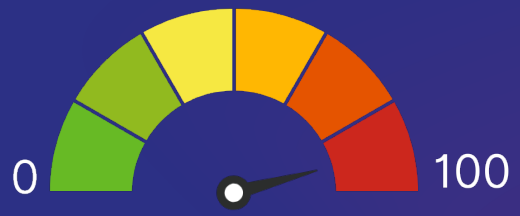
- Reduced costs
- Flexibility
- ~~Plausible deniability~~
- Efficiency

# CHINA: Vulnerability identification and exploitation strategy

# RUSSIA – CHINA: A comparative analysis

| Proxy Characteristics / Countries |  |  |
|---|---|---|
| Private companies | YES | YES |
| Degree of autonomy of private companies | MEDIUM-LOW | HIGH |
| Full outsourcing to private companies | NO | YES |
| Hacktivist groups | YES | UNCLEAR |
| Independent hackers | YES | NO |
| eCrime groups | LIKELY | NO |
| Information operations | FOREIGN | DOMESTIC |

# THE PROXY WARFARE: Conclusions




**Efficient**

**+**

**IMPLAUSIBLE DENIABILITY**

**=**

**FLOURISHING INDUSTRY**

**Increasingly complex environment**

**Challenging attribution**