**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# 2019 GRU defacement of Georgian Government, courts, NGOs, media, businesses, and national broadcasters websites

## Summary

The GRU conducted a wide-ranging cyber-attack that interrupted the service of several national broadcasters and defaced approximately 15,000 websites belonging to Georgian government, non-government, and private sector entities. The Kremlin launched a multichannel strategy using official diplomatic channels, Kremlin-funded media, fringe outlets, and pro-Kremlin outlets within Georgia to widely spread Russia's narrative: dismiss, deny, and deflect. Using a range of diverse media sources, coupled with the reinforcement of its plausible deniability arguments, is designed to create the impression that Russia’s version of events is more authoritative. Georgian authorities were accused of obstructing political stabilisation between Russia and Georgia. Around 20 countries condemned Russia’s act of cyber aggression against Georgia, stressing that it was part of the Kremlin’s long-running campaign to destabilise Georgia and an attempt to sow discord ahead of the 2020 Georgian parliamentary elections.

## Timeline and Context

October 2019

* On or about October 28, 2019, the Conspirators engaged in a wide ranging cyberattack against a large number of entities in the country of Georgia.
  + This attack targeted websites belonging to Georgian government, non-government, and private sector entities and involved the defacement of approximately 15,000 websites and the disruption of service to some of these websites after the computer systems of a Georgian web hosting provider were compromised. In many cases, the Conspirators replaced website home pages with an image of a former Georgian president, who was known for his efforts to counter Russian influence in Georgia, along with the caption "I'll be back."
  + Initial targets of the attack included state agencies, media outlets, and non-governmental organisations.
  + Following those attacks, local hosting provider ProService reported that 15,000 websites were disabled after their servers were attacked by hackers.
* Russia’s long-running campaign of hostile and destabilising activity against Georgia.
  + The Kremlin unleashed a multi-channel counter-messaging campaign after it had been made clear Russia’s GRU was behind the attack.
  + The Russian Ministry of Foreign Affairs was first to dismiss the attribution, which was later amplified by Russian diplomatic social media accounts and then large Kremlin-funded outlets. Amplification of anti-Western narratives continued with Russian fringe media outlets and pro-Kremlin Georgian media outlets.
* Irakli Chikhladze, head of news at TV station Imedi, posted on Facebook that there was no signal, and the station was unable to broadcast.
  + Both Imedi and another network, Maestro, were affected, he said. Imedi TV was paralysed for under an hour while Maestro's computers and other equipment were reportedly damaged or destroyed.
* Another network, Maestro, reported that some computers and other equipment were damaged or destroyed.

## Frameworks

### ATT&CK Framework

* **TA0043 Reconnaissance**
  + T1595 Active Scanning
  + T1591 Gather Victim Org Information
    - T1591.002 Business Relationships
      * Information about an entities business relationships may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.). This includes the Georgian web hosting provider ProService.
  + T1594 Search Victim-Owned Websites
    - Victim-owned websites may contain a variety of actionable information including  business operations and relationships.
* **TA0042 Resource Development**
  + T1650 Acquire Access
  + T1584 Compromise Infrastructure
    - T1584.004 Server
      * ProService servers were attacked.
* **TA0040 Impact**
  + T1499 Endpoint Denial of Service
  + T1491 Defacement
    - T1491.002 External Defacement

### DISARM Framework

* **PLAN**
  + TA01 Plan Strategy
    - T0073 Determine Target Audiences
    - T0074 Determine Strategic Ends
  + TA02 Plan Objectives
    - T0002 Facilitate State Propaganda
    - T0075 Dismiss
      * T0075.001 Discredit Credible Sources
  + TA13 Target Audience Analysis
    - T0072 Segment Audiences
      * T0072.001 Geographic Segmentation
      * T0072.005 Political Segmentation
    - T0080 Map Target Audience Information Environment
      * T0080.005 Assess Degree/Type of Media Access
    - T0081 Identify Social and Technical Vulnerabilities
      * T0081.008 Identify Media System Vulnerabilities
* **PREPARE**
  + TA14 Develop Narratives
    - T0003 Leverage Existing Narratives
    - T0004 Develop Competing Narratives
    - T0040 Demand insurmountable proof
    - T0068 Respond to Breaking News Event or Active Crisis
    - T0083 Integrate Target Audience Vulnerabilities into Narrative
  + TA06 Develop Content
    - T0019 Develop Image-based Content
  + TA15 Establish Social Assets
    - T0091 Recruit Malign Actors
      * T0091.002 Recruit Partisans
    - T0095 Develop Owned Media Assets
  + TA16 Establish Legitimacy
    - T0100 Co-opt Trusted Sources
  + TA05 Microtarget
    - T0101 Create Localized Content
* **EXECUTE**
  + TA09 Deliver Content
    - T0115 Post Content
    - T0117 Attract Traditional Media
  + TA17 Maximize Exposure
    - T0118 Amplify Existing Narrative
  + TA18 Drive Online Harms
    - T0123 Control Information Environment through Offensive Cyberspace Operations
      * T0123.002 Block Content
      * T0123.003 Destroy Information Generation Capabilities
  + TA11 Persist in the Information Environment
    - T0060 Continue to Amplify
    - T0129 Conceal Operational Activity
      * T0129.003 Break Association with Content
      * T0129.006 Deny Involvement
    - T0130 Conceal Infrastructure
      * T0130.004 Use Cryptocurrency
      * T0130.005 Obfuscate Payment
  + TA12 Assess Effectiveness
    - T0132 Measure Performance
      * T0132.002 Content Focused
    - T0133 Measure Effectiveness
      * T0133.001 Behaviour Changes
      * T0133.002 Content
      * T0133.003 Awareness
      * T0133.004 Knowledge
      * T0133.005 Action/Attitude
    - T0134 Measure Effectiveness Indicators (or KPIs)
      * T0134.001 Message Reach
      * T0134.002 Social Media Engagement

## Resources

## [Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment]( 2020\_10\_19\_unsealed\_indictment\_0.pdf)

## [NY Times](https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html#:~:text=The%20cyberattack%20took%20out%20internet,high%20number%20of%20empty%20seats)]

## [RAND](https://www.rand.org/pubs/commentary/2018/02/why-the-2018-winter-olympics-are-the-perfect-storm.html)

## [WIRED](https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/)

## [IT News](https://www.itnews.com.au/news/winter-olympics-suffers-cyber-attack-484949)

## [Cyberlaw](https://cyberlaw.ccdcoe.org/wiki/Olympic\_Destroyer\_(2018))