

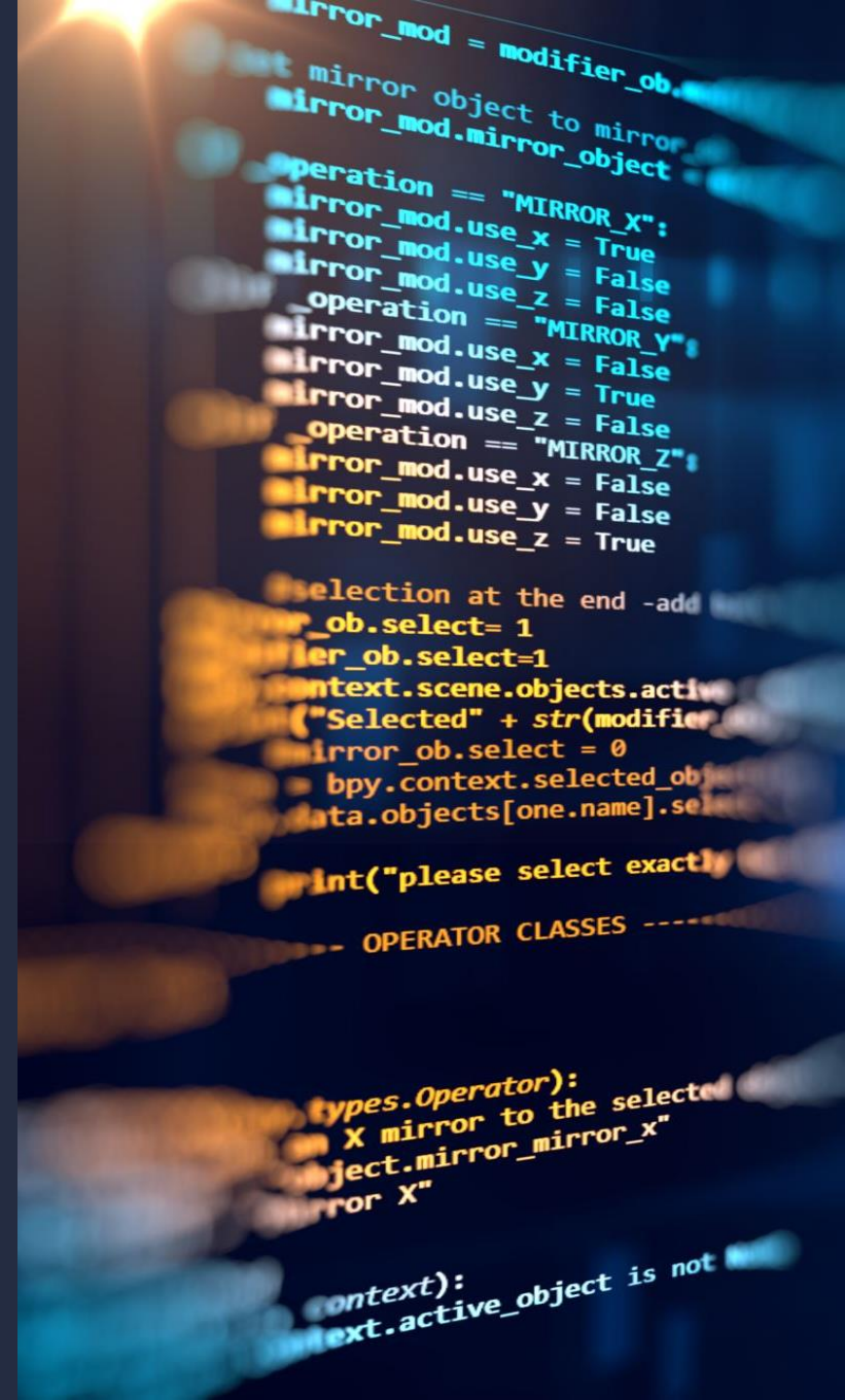


GAMING HYBRID WARFARE CYBER OPERATIONS

DR. ROGER MASON



LECMgt





WHAT IS HYBRID WARFARE?



CYBER-ENABLED OPERATIONS

How we

- Think
- Plan
- Communicate
- Fight



CURRENT LEADER IN TACTICAL CYBER OPERATIONS?

RUSSIA

The Russians have deployed offensive cyber actions during hybrid warfare operations.
(Vladislav Surkov)

- Estonia 2007
- Georgia 2008
- Crimea 2014
- Syria 2017-18

FOUR LEVELS OF RUSSIAN TACTICAL CYBER

- **Battalion Tactical Group**
- **Special Ops**
(Spetsnaz, “Little Green Men.”)
- **Proxies** (Night Wolves, protestors, contractors)
- **Agents**





HOW TO DESIGN A GAME WITH TACTICAL CYBER

THE BATTLE OF VORU



BATTLE OF VORU

- A hypothetical scenario involving a Russian hybrid warfare attack on southern Estonia. The objectives include capturing a corridor isolating Estonia from Latvia and destroying a US Air Force Global Hawk base in Voru.



START WITH FOUR BACKGROUND ASSESSMENTS

The combatants:

- **The kinetic capabilities.**
- **The cyber capabilities.**
- **Operational cyber requirements.**
- **Rules of engagement.**

KINETIC CAPABILITIES

NATO Battalion Task Force

Estonian Defense Forces, Police/Militia
Forces

Russian Forces

- Battalion Tactical Group
- Special Ops: Spetsnaz
- Proxies: Protestors, Night Wolves





CYBER CAPABILITIES OF THE COMBATANTS

- **NATO:** Cyber is used to optimize conventional operations and prevent electromagnetic spectrum attacks.
- **Estonia:** Use cyber for communications. They adapt commercial applications to support operations. They have specialized cyber defense units.
- **Russians:** Primary offensive capabilities.



CYBER REQUIREMENTS

- **NATO:** Relies on a high level of cyber support
- **Estonia:** Uses cyber for communication, technology and capability work-arounds.
- **Russians:** Have very limited cyber requirements

RULES OF ENGAGEMENT

- **NATO:** NATO follows the Geneva Convention and the International Humanitarian law. This includes cyber operations.
- **Russia:** To achieve the objective any operation or action is permissible.



BATTLE OF VORU: THE RUSSIANS

- The Russian conventional forces are organized into battalion tactical groups.
- The Russians have the option of grey-area operations prior to conventional attacks. They can conduct cyber attacks against Estonian and NATO forces.
- The Russians can attack critical infrastructure to degrade wireless communications, public information, and electrical utilities.
- Russians can employ their proxies to shield their maneuver forces or block NATO forces.



BATTLE OF VORU: NATO

- NATO forces have special forces in place as a trip wire.
- Estonia civil forces can confront proxy operations
- NATO units have limited Cyber Electromagnetic Activities (CEMA) teams.
- The Estonian forces have specialized cyber defense units.



BATTLE OF VORU

The game includes:

- UAVs
- Air Operations
- Civilians





EXAMPLE OF PLAY

- Russians forces have deployed a rolling barrage blacking out wireless communications in front of their forces.
- They have launched a logic persona attack on an Estonia unit.

QUESTIONS?

Roger Mason, PhD

LECMgt

340 Rosewood Ave Suite J

Camarillo, Ca 93010 USA

roger@lecmgt.com

818 693 1668



LECMgt

