Military Advantage (MA)
Europe (EU)
NATO Member (NM)
Cyber Influence (CI)
Cyber Disruption (CD)
Covert Military Intervention (COVM)
Overt Military Intervention (OVM)

Additional notes
criminality/cybercrime networks → where does it fit? (cf. NYT conjecture below that RBN perpetrated DDoS attacks in Georgia in August 08)

GEORGIA (2008)
MA
[*proposed NM*]
CI
CD
COVM
[COVM not incl. in Prof. Lindsay's original table for Georgia; but cf. M. Carpenter's SASC testimony[1] and Galeotti 2016 ECFR article[2] citing July 20 cable[3] on Russian active measures from US Amb. Tefft]
OVM

TIMELINE
5/2/08: Presidential election in Georgia takes place following incumbent Mikheil Saakashvili's resignation over criticism of suppressing political dissidents; Saakashvili re-elected with 53.47% of vote on platform of corruption reduction, poverty reduction and **territorial integrity**[4]

1/2/08: Bremmer predicts hostile Russian activity toward Georgia over secession-oriented Abkhazia[5]

[1] https://www.armed-services.senate.gov/imo/media/doc/Carpenter_03-29-17.pdf
[2] http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf
[3] https://wikileaks.org/plusd/cables/07TBILISI1732_a.html
[4] https://fas.org/sgp/crs/row/RS22794.pdf
[5] https://www.terrafirma.com/an-alternative-perspective-article/items/five-other-top-global-risks-for-2008.html

3/4/08: Bucharest Summit Declaration (NATO) welcomes Ukraine's and Georgia's aspiration to join the alliance, "…We agreed today that these countries will become members of NATO." (par. 23)[6]
*_this announcement made only one month before 2008 parliamentary elections in Georgia (**were cyber tools deployed?**) and 4 months prior to OVM beginning August_

6/5/08: Letter from Irakli Alasania (Perm. Rep. of Georgia to UN) outlines misinformation for possible justification of Russian mil. action against Georgia; false claims by Russian FM that Abkhaz separatists shot down unarmed Georgian UAV in security zone[7]
(evidence of CI; evidence of COVM?)

18/7/08: Shadowserver group observes initial DDoS attack against Georgian president, Mikheil Saakashvili (evidence of ICMP flood, TCP SYN flood, HTTP flood); website disabled/extremely slow for several days; Shadowserver concludes requests were issued by a **Machbot** controller that had over 15,000 bots[8]

20/7/08: date Russian cyber operations begin, according to 14/8/08 interview with Weekly Standard senior writer, Stephen Hayes on CNN Situation Room[9]

to be developed…OVM (air/land/sea) trad. mil. conflict timeline [UN Yearbook has a good one]

8/8/08: CD begins at higher level of intensity than previously[10]

10/8/08: RIA Novosti website disabled on 3rd day of OVM ***(hackback?)***[11]

10/8/08: Analysis by Renesys (acquired by Dyn in 2014) links internet connectivity to physical infrastructure (**i.e. pipelines**) and physical terrain, noting Georgia's limited options; main findings:

- Georgia has 309 prefixes (networks) run from 24 autonomous systems
- over conflict period Aug. 7 to 10 ~35% of networks disappeared from internet for extended periods and ~60% unstable; **nothing permanent**
- land route connectivity through Turkey, Armenia, Azerbaijan, Russia; most of 309 prefixes routed through Turkey TTnet or Azerbaijan's Delta Telecom, **which is ultimately linked to Russia via TransTelCom**; Renesys did not observe routing changes during conflict, notes most traffic transits Turkey

[6] http://www.nato.int/cps/en/natohq/official_texts_8443.htm?selectedLocale=en
[7] http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2008/299
[8] https://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf
[9] https://global-factiva-com.myaccess.library.utoronto.ca/redir/default.aspx?P=sa&an=CNNTSR0020080815e48e00001&cat=a&ep=ASE
[10] https://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf
[11] https://sputniknews.com/russia/20080810115936419/

- Georgia has just completed first stage of **direct undersea cable connection to Europe** via Bulgaria[12]

11/8/08: Shadowserver group summarizes CD since 20/8/08, noting groups targeting Georgian websites have also been targeting Russian websites; commentary includes remark on defacement [**evidence of CI**] of Georgian Parliament website (pictures of Georgian President placed in mosaic with Hitler; act allegedly carried out by South Ossetian group); remarks on changes of Georgian IP addresses, including to Atlanta, GA (Tulip Systems web hosting)[13]

12/8/08: Arbour Networks – early observers of CD – report on RIA Novosti shutdown, but say no evidence of state sponsorship of CD on either side, though Georgian hackers were accused of RIA shutdown[14]

12/8/08: NYT article covers DDoS event in Georgia, crediting Arbour Networks and Shadowserver with first reporting CD[15]

- also notes, "According to Internet technical experts, it was the first time a known cyberattack had coincided with a shooting war."
- also notes defacement of Georgian Parliament and National Bank of Georgia websites
- also notes attribution difficulty: official deployment of kinetic force does not necessarily mean cyber ops officially directed ***(Shadowserver group also warns against this confirmation bias – suggests Russian authorities might have inspired attacks rather than controlled them)***[16]
- also notes possible involvement of Russian Business Network (St. Petersburg criminal network)
- also notes evidence of internet traffic redirected through Russian telecoms firms in week prior to invasion; software signature in attacks traceable to these firms
- also notes, "A Russian-language Web site, stopgeorgia.ru, also continued to operate and offer software for download used for D.D.O.S. attacks."
- also notes, "…in the run-up to the start of the war over the weekend, computer researchers had watched as botnets were "staged" in preparation for the attack, and then activated shortly before Russian air strikes began on Saturday."

13/8/08: Shadowserver group posts update of Georgia conflict, noting possible parallel to Estonia (2007); Russian blogs, forums, etc. sharing Microsoft Windows batch script and encouraging people to send ICMP traffic with a 'ping' command to (mostly)

[12] http://dyn.com/blog/georgia-clings-to-the-net/
[13] http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811
[14] https://www.arbornetworks.com/blog/asert/georgia-ddos-attacks-a-quick-summary-of-observations/
[15] http://www.nytimes.com/2008/08/13/technology/13cyber.html
[16] https://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf

Georgian government websites; conclusion – sympathetic computer users involved in overwhelming Georgian websites, high skill level not req. – “grass roots effect”[17]

13/8/08: NYT article speculates on **oil dimension** of Russo-Georgian conflict, citing possibility of decreased reliance on Russian oil transportation infra. as possible driver of Russian action, “[t]he building of the pipeline that passes through Georgia, the Baku-Tbilisi-Ceyhan line, or BTC, remains one of the signature successes of the American strategy to put a wedge between Russia and the Central Asian countries that had been Soviet republics.”[18]

14/8/08: FP interviews Eurasia Group expert, Clifford Kupchan, who says Russia pursuing multiple objectives in Georgia:

1. **Signalling** – NATO accession v. risky for former USSR satellites
2. **Regional influence** – Caucasus is firmly in Russian sphere
3. **Energy** – high risk associated with Caucasus energy corridors that exclude Russia[19]

15/8/08: Renesys (Dyn) research blog notes sudden and extensive **network outage** that geo-locates to Georgia, speculating cause to be extensive power failure; comes after week of relative stability; >68% originate with local DSL provider, United Telecom of Georgia; restored same day, but remained unstable[20]

16/8/08: ABC reports oil transportation agreements favourable to EU and US may have increased Georgian vulnerability to Russian interference – “safe route” not safe; but also, **BTC pipeline was down** prior to commencement of Russian OVM on Aug. 8 (due to alleged PKK sabotage along Turkish section on pipeline cf. Reuters note below [article from 28/8/08])[21]

20/8/08: TrendMicro posts analysis of malware enclosure in news spam related to Russia-Georgia conflict; users directed to view “shocking video” from the conflict at a website, but link executes malicious file identified as TROJ_XCHANGER.B instead[22]
(contextualized in current events but opportunistic – targeted or random?)

21/8/08: TrendMicro reports similar spamming activity, this time with password-protected .ZIP file (*this apparently prevents e-mail filters from scanning attached files for malicious content*) that recipients are invited to open to view Turkish journalists from NTV being shot at while reporting near Gori; .ZIP file identified as WORM_DLOAD.RAR

[17] https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080813
[18] http://www.nytimes.com/2008/08/14/world/europe/14oil.html
[19] http://foreignpolicy.com/2008/08/14/seven-questions-russia-plays-realpolitik-with-bare-knuckles/amp/
[20] http://dyn.com/blog/georgia-on-my-mind-1/
[21] http://abcnews.go.com/Business/story?id=5595811&page=1
[22] http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-spammers-leverage-russian-georgian-conflict/

and attachment when opened executes as TROJ_DLOADER.UAF, which downloads program to present fake virus warnings before directing victim to buy fake antivirus program[23]
(behavioral exploit – again, targeted or random?)

29/8/08: one outcome of hostilities: **possible reroute of Azeri oil and gas through Russia** via Baku-Novorossiisk link instead of BTC pipeline, "On August 7, Socar [Azerbaijan energy firm] asked Azeri pipeline operators to reroute some of its crude volumes through Russia -- the same day that Georgian troops stormed Georgian breakaway region South Ossetia, provoking a huge counter-response from Russia."[24]

3/12/08: NATO communiqué condemns Russia's "**disproportionate**" military actions in Georgia – BAU NATO-Russia relations suspended

- ALSO, "We call upon Russia to refrain from confrontational statements, including assertions of a sphere of influence, and from threats to the security of Allies and Partners…"[25]

28/4/09: NYT article references Estonia and Georgia DDoS in context of US crit. infra. vulnerability, concluding these 2007 and 2008 ops did **no lasting damage**.[26]

8/09: US-CCU report analysis highlights several features of the cyber campaign against Georgia **not widely reported elsewhere**:

1. importance of social networks for recruitment
2. evolution of methods since Estonia 2007 (i.e. effect of HTTP tools much greater than ICMP observed in Estonia)
3. customization of attack toolkit
4. premeditation – clue given by creation of defacement graphics 2 years prior
5. physical destruction of Georgian comms and media facilities avoided b/c cyber tools v. effective
6. Estonia-Georgia cooperation[27]

to be developed…fallout and attempt to reshape norms and behavior (esp. by NATO) + technical analyses released in aftermath + linkages to lesser known cases

---

[23] http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-russian-georgian-spam-uses-zip-password/
[24] http://www.reuters.com/article/us-caucasus-europe-oil-idUSLT62498120080829
[25] http://www.nato.int/cps/on/natohq/official_texts_46247.htm?selectedLocale=en
[26] http://www.nytimes.com/2009/04/28/us/28cyber.html
[27] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

POSSIBLE CAUSES

- Development of Caspian Sea oil supply routes through Georgia regarded as hostile by Russia – weakening Russian monopoly on supply to Europe
- Disrupt NATO enlargement (encirclement?) plans → attempt to put Georgia's military reform benchmarks req. for full NATO membership out of reach
- Expansion of "sphere of influence"
    - Territorial dimensions → logic of liberating Russians inside foreign territory (Abkhazia & South Ossetia) from oppressive regime//arguments used in Ukraine & Crimea
- Information and connectivity; reinforce Georgian dependency on Russian internet infrastructure → monitoring; maintaining pathway for future disruption; intelligence interception

THEORY of INFERRING CAUSES (and PREFERENCES)
developed from: Frieden and Lake, Yarhii-Miro, Cimbala, Schelling

OTHER EVENTS
Kyrgyzstan:
Since January 18, 2009, the two primary Kyrgyzstan ISPs (www.domain.kg, www.ns.kg) have been under a massive, sustained DDoS attack almost identical in some respects to those that targeted Georgia in August 2008. Few alternatives for Internet access exist in Kyrgyzstan. With just two smaller IPSs left to handle the load, these attacks from Russian IP address space have essentially knocked most of the small, Central Asian republic offline."[28]

Lithuania?
Kazakhstan?
Belarus?

[28] https://www.secureworks.com/blog/research-20957