Hybrid Conflict

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael
Netherlands Institute of International Relations

Novel and Important Signals to Watch: Threats and Opportunities

- **Non-state proxy organizations are becoming more important in waging hybrid conflict**
    - Russian paramilitary organizations, such as the Wagner Group, are covertly deployed worldwide to manipulate elections and exercise pro-Kremlin influence. (Hybrid COE, Meduza)
    - Criminal groups linked to the Chinese Communist Party have been attacking pro-democracy protesters in Taiwan, emulating Kremlin tactics used since Soviet times. (International Affairs Blog, Moscow Times)
    - States increasingly rely on cybercriminals as extensions of state power in cyberspace, as evidenced by the activities of groups such as Advanced Persistent Threat 41 (China) and The Mabna Institute (Iran). (ISPI, Wall Street Journal, RAND, Nikkei Asian Review)
    - *Which steps can the EU take to curb this subtle but visible interference with democratic societies?*
- **Modern societies' dependence on the Internet of Things increases the attractiveness of hybrid tactics as a force multiplier**
    - The expansion of cyberspace and artificial intelligence (AI) enhances the opportunity for exploitation and damage. (IntechOpen, China's National Defense in the New Era)
    - Communications companies are increasingly being used as proxies by state intelligence services. (CCDCOE, Haaretz)
    - 5G networks hold the potential for exploitation and may disrupt NATO force deployment (National Interest, Gestion [Peru], Cyber Security Agency of Singapore, Financial Times)
    - *How can states become resilient against cyber threats without losing the advantages and freedoms of cyberspace?*
- **States' perceptions of critical infrastructure and the role of private actors is changing**
    - New awareness of the role of private entities (such as DigiD, Facebook) in providing critical public services has prompted the formulation of numerous regulation and protection mechanisms. (The Guardian, Technology Review, NRC)
    - Recent pre-EU election measures, such as fake account removal, disinformation detection and the amplification of fact-checked content, show that information campaigns are now part and parcel of national preparations. (European Parliament, Bloomberg)
    - Nigeria and India are now awakening to the societal impact of fake news spread via Facebook and Twitter, which is stoking ethnic and religious rivalries to influence elections. (ISPI, Quartz India)
    - *What other 'soft spots' exist in our society that could be classified as critical infrastructure?*
- **Economic coercion is being employed more overtly**
    - Tensions between the US and China and between India and Pakistan have resulted in overt economic coercion. (Global Times China, Financial Times, Business Today India)
    - Anxiety over China's influence operations through telecommunications companies has grown amid concerns over Beijing's manoeuvres in foreign states. (RAND, Washington Post, Ambito Financiero)
    - Beijing offers large incentives for Chinese students to attend foreign universities, facilitating the transfer of information and technology. (New Oriental Network)
    - *How can the EU shield itself against the impact of economic coercion?*
- **Military exercises near borders have become commonplace, increasing the chance of escalation**
    - Video and satellite imagery show Chinese military troops massing near the border with Hong Kong during the recent protests. (France 24, Japan Times)
    - Iran's top security body has labeled sudden US moves to send an aircraft carrier and bombers to the Middle East a form of "psychological warfare" (The Guardian, Tasnim News Agency)
    - Immediately following news of Turkey's intentions in North Eastern Syria, Iran began conducting military exercises along Turkey's border. (RadioFarda, The Jerusalem Post)
    - *How can this form of influence and posturing be minimized, e.g. through code of conducts or transparency building measures on multilateral levels?*

Hybrid Conflict

Global Security Pulse, Strategic Monitor 2019–2020

Long-Term Trends: Hybrid Conflict

Multi-factor Trend Assessment (10-year timespan)

	Trends	
Perception	States' perception of hybrid conflict as a threat to their national security	▲
	States' intention to use hybrid means as part of their defense strategies	▲
Capability	Capacity of states to engage in and/or respond to hybrid conflict	▲
Military Activity	The use of proxies by state actors in third party military conflicts	▲
	Military exercises near borders	▲
	Aerial and maritime intrusions	▲
Political Activity	External meddling in domestic politics	▲
Economic Activity	Economic coercion	▲
Information Activity	Disinformation campaigns	▲
Civil Activity	Cyberattacks on critical infrastructure	▲

▲ Increase
▬ Stable
▼ Decrease

🟥 Increase threat
🟩 Decrease threat

Hybrid Conflict

Global Security Pulse, Strategic Monitor 2019–2020

Novel and Important Signals to Watch: The International Order

- **The countering and deployment of hybrid tactics is becoming mainstream within the EU and NATO**
  - On national and multilateral levels, states are forming new military divisions, specialized working groups, and committees to prepare for potential confrontations. (Independent, eu2019.fi, EU Observer, China's Defense White paper 2019, Dialogo Americas Peru)
  - In retaliation to Iran's downing of an American drone, the US opted to call-off military retaliation in favor of cyberattacks against Iranian rocket launch systems. (Reuters, The Times of Israel, Al Jazeera)
  - NATO leaders maintain that NATO's Article 5 common defense obligation can be triggered in the case of a hybrid attack and continue to train Counter Hybrid Support Teams (Atlantic Council)
  - *How can these policy-driven counter-efforts be incorporated into day-to-day operations at the practical level?*
- **EU institutions are evaluating the potential of new technologies to counter hybrid conflict**
  - Machine Learning (ML) will play a crucial role in processing information into actionable intelligence and may facilitate 'AI to fight AI' solutions. (c4isrnet, Carnegie, CSF, Instituto de Estrategia Internacional)
  - The EU Cybersecurity Certification Framework promotes a security-by-design approach, which urges producers and providers of tech to anticipate and minimize threats during the earliest development stages. (IACS, EEAS)
  - *What stance will the EU take in defining guidelines for AI technologies in defensive contexts?*
- **States, institutions and companies are stepping up efforts to shield the energy sector from hybrid threats**
  - Given modern society's growing dependence on energy, the EU Commission and the US are acknowledging the need to reduce Europe's dependence on Russian energy. (Strategic Studies Institute)
  - Eastern EU member states have been active in forging their own energy and infrastructure organizations, thus diverging from the German and French positions. (The Polish Institute of International Affairs, Carnegie Endowment, DW)
  - Siemens and Chronicle have announced a partnership to protect the energy industry's critical infrastructure from sophisticated cyber threats. (VentureBeat)
  - *How can the EU become less dependent on Russia's energy supply and form a unified approach to Russian partnerships?*
- **Efforts to counter disinformation and electoral interference at the EU and national levels are materializing**
  - Preparation for the 2019 EU elections involved deleting fake accounts, labelling messaging activities by bots, amplifying reliable content, and cooperating with fact-checkers to detect disinformation. (European Parliament, Bloomberg)
  - Social media companies have implemented new tools geared towards mitigating the impact of disinformation and election manipulation. (Washington Post, Verge)
  - The European Commission has more than doubled its spending on counter-disinformation this year to five million euros. (Bloomberg)
  - *How can the policymaking cycle be amended to allow it to keep up with ever-evolving hybrid tactics?*
- **Stronger public and private governance arrangements are being forged in support of deterrence of cyber threats**
  - Newly forged public-private partnerships are endemic of the private sector's growing role in mitigating cyber threats. (EEAS, World Economic Forum, GCSC, OpenGovAsia)
  - An EU-funded project was approved in 2019 with the aim of improving cyber resilience in the Eastern Partnership countries and enhancing cooperation between public authorities and private entities. (EEAS)
  - *How can public-private cooperation efforts in the cyber domain be further extended to counter other hybrid threats?*

Hybrid Conflict

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael
Netherlands Institute of International Relations

Long-Term Trends: Development of the International Order

Multi-year Regime Analysis (10-year timespan)

Norms	Trend	Rules	Trend
Norm of state accountability for their non-state actor partners	▼	States are responsible for the conduct of the proxy actors they control (Article 8, Responsibility of States for Internationally Wrongful Acts, 2001)	▼
Norm of non-interference in other states' election processes	▼	States should not interfere with the internal affairs of another state, including publicizing the outcome of espionage campaigns to influence an election and targeting critical electoral infrastructure	▼
Norm of open, non-discriminatory trade between states	▼	States cannot normally discriminate between their trading partners (Article 1, GATT 1994)	▼
Norm of non-interference in other states' societal discourse	▼	States should not interfere with the internal affairs of another state, including the use of false propaganda to influence foreign electoral processes or create civil disarray	▼

▲ Increase
▬ Stable
▼ Decrease

🟥 Increase threat
🟩 Decrease threat

Authors: *Bianca Torossian, Tara Görder, Lucas Fagliano (HCSS).* ***Contributors:*** *Tim Sweijs, Hugo van Manen, Dylan Browne-Wilkinson (HCSS), Danny Pronk (Clingendael)*

For a general methodological justification of horizon-scanning click here and for the methodology document specific to 'Hybrid Conflict' click here. A Research Paper that further explains and analyzes the trends shown in the two Long-Term Trend tables of this Global Security Pulse will be published in November 2019.

Disclaimer: *The Global Security Pulse is part of the PROGRESS Program Lot 5, commissioned by the Netherlands' Ministries of Foreign Affairs and Defense. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.*