

A HORIZON SCAN OF TRENDS AND DEVELOPMENTS IN HYBRID CONFLICTS SET TO SHAPE 2020 AND BEYOND

TNO innovation
for life

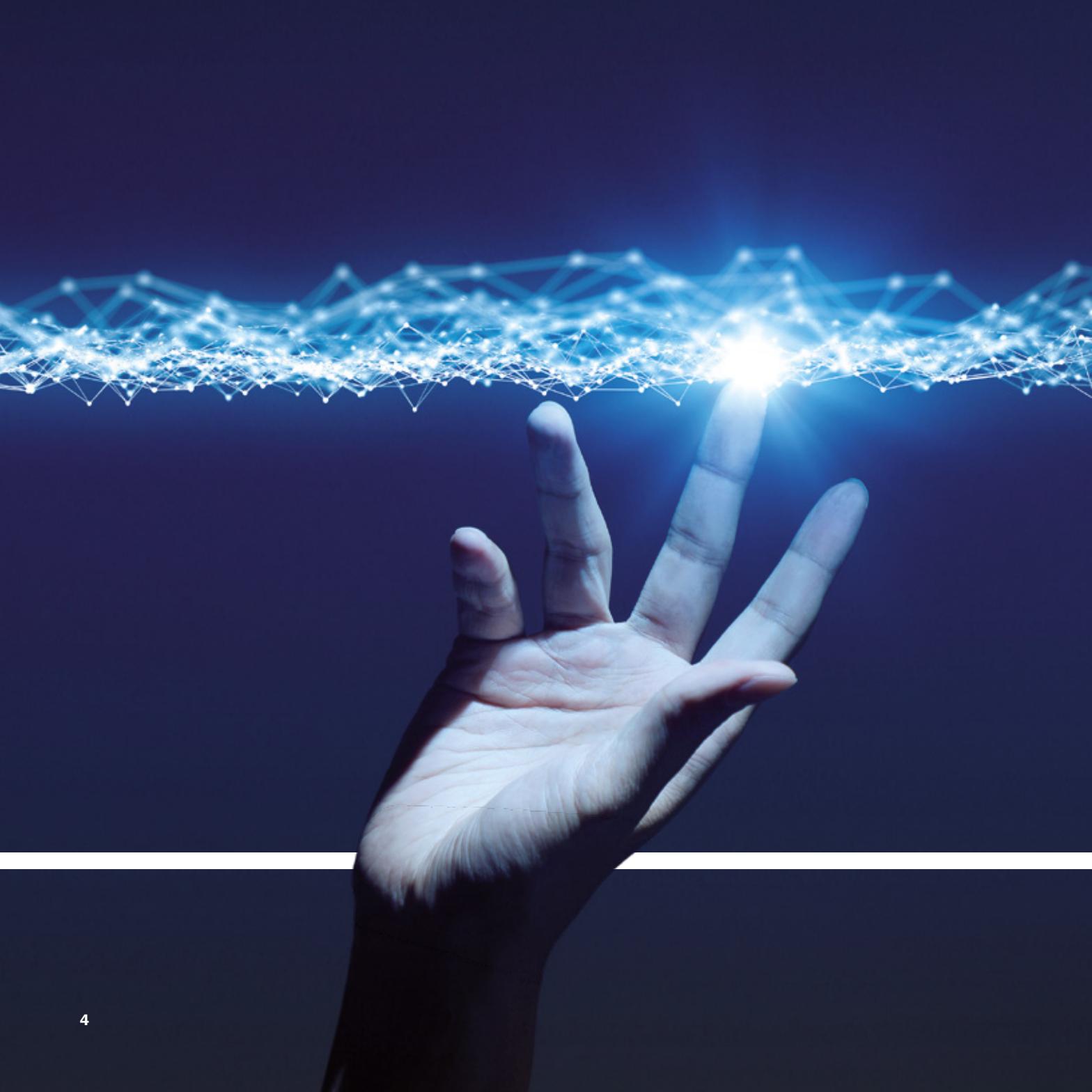


Rick Meessen (TNO)
Bianca Torossian (HCSS)
Frank Bekkers (HCSS)

TABLE OF CONTENTS

Foreword	5
1 Introduction	7
2 Trends and Developments in Hybrid Campaigns	8
2.1 Globalization of Hybrid Threats	8
2.2 Private Roles in Public Goods	10
2.3 Rise of Lawfare	12
2.4 Special Ops Operatives	13
2.5 Military Exercises as 'Psychological Warfare'	14
2.6 Economic Sticks, Carrots and Sledgehammers	15
2.7 Hiding behind Proxies	17
2.8 Political Machinations	20
2.9 Shifting Realities	20
2.10 Formation of Digital Islands	22
2.11 Cyberspace: The Fragile Underbelly of Society	23
2.12 Emerging Technologies: Amounting to New Capabilities	24
3 Emerging Technologies and Capabilities in Hybrid Threats	27
3.1 The Why and What of Emerging Technologies	27
3.2 Additive Manufacturing	30
3.3 Unmanned and Autonomous Systems	31
3.4 Extended and Synthetic Reality	32
3.5 Internet-of-Things and 5G Network Technology	34
3.6 Satellite Jamming, Spoofing and Hacking	36
3.7 Offensive Cyber Tools	37
3.8 Micro and Precision Targeting	39
4 Synthesis	42

This booklet is a product of the research program “Resilience to Hybrid Threats (V1925)”. The authors would like to thank Tara Görder and Lucas Fagliano (HCSS) and Carolina van Weerd (TNO) for their role in conducting background research necessary for this booklet.



FOREWORD

Hybrid conflict entails gaining influence, with all possible visible and invisible means, below the threshold of armed conflict. Not only great powers use hybrid instruments, skirting the boundaries of full-blown conflict, but increasingly also smaller states and non-state actors. This injects additional risks of misinterpretation and escalation into the already complex arena of international relations and conflicts. It is not just 'others' that are to blame; some Western democracies also conduct hybrid campaigns, or at least activities that can be interpreted by the receiving end as such (cf. the view of the Kremlin on NATO's enlargement process in the nineties). This provides room for opponents to argue that they only do to us what we do to them. In short, hybrid threats are here to stay. Not in the least because large scale interstate armed conflict is (presently) considered too costly by friend and foe alike, and hybrid actions offer a relatively low-cost, high-gain alternative to pursue national interests.

Especially smaller nations, being more dependent on a rule-based international order, should have a strategy on how to recognize, understand and manage hybrid threats in order to retain (shared) sovereignty. Effectiveness of such a strategy today, however, does not ensure its effectiveness tomorrow. Instruments and technology develop with ever increasing speed. Countermeasures against hybrid threats can therefore only be timely implemented by actively and constantly exploring new trends and developments.

This paper serves as a first iteration of a horizon scan of trends and developments in hybrid threats set to shape 2020 and beyond, based on open source information with a cut-off date of December 2019. In view of the exponential development of instruments and technology, scans like this should be periodically repeated. Its results should be discussed between researchers, operators and policy makers in order to establish the 'so what' and 'what if' of each trend as the basis for timely design and implementation of resilience against hybrid threats (organization, processes, technology). That is conditional for being master of our own destiny as much as practically possible.

Rear admiral (rtd) Pieter Bindt
Former Director Netherlands Defence Intelligence and Security Service



INTRODUCTION

Hybrid conflict is the coordinated use of conventional and unconventional activities that state or non-state actors use to achieve political outcomes.¹ Hybrid threats are characterized by their complexity, ambiguity, multidimensional nature and gradual impact. Hybrid instruments include conventional military activity, interference with political processes, the use of economic coercion, the proliferation of disinformation campaigns and cyberattacks on critical infrastructure. The challenge in countering hybrid threats is that the tactics deployed are slow burning and executed under the threshold of armed conflict, making them difficult for states to effectively respond to. A concealed hybrid action may hardly appear on the radar, until the seemingly isolated event is put into context as part of a state's broad tapestry of activities designed to undermine adversaries.

Hybrid threats are one of the main challenges Western democracies currently struggle with.² Hybrid threats are in the news, mostly framed or wrapped in specific 'hybrid' phenomena such as disinformation, foreign meddling in elections and cyber hacks. Governments warn us about them. Institutions like NATO and the EU write policy papers and organize symposia and workshops to discuss them. Various security providers are in the process of defining strategies and developing capabilities to counter hybrid threats, mostly in a particular incarnation rather than across the board. The ultimate response to hybrid threats has not been found and in all likelihood does not exist. Countering those threats will remain a very challenging task as long as hybrid threats will evolve due to technological advances and new ways of hybrid campaigning.

This horizon scan, based on literature and media scanning, expert sessions and information exchanges with international peer institutes, captures some of the current and emerging trends and developments in hybrid conflicts and threats. It highlights both the evolution of hybrid campaigns and elements used in these campaigns, illustrated by some examples in Chapter 2, and current and new technologies that will or might change the hybrid 'battlefield' in Chapter 3.

We do not pretend to be complete. Our aim is to provide to a wider audience an overview of some of the most salient trends and emerging technologies likely to influence hybrid threats, tactics and activities. Further note that a scan of trends and developments can also be performed with counter strategies – how to prevent, monitor, detect and counter hybrid threats – in mind. This is a very valid and useful approach, but not the main driver for the selection presented here that is primarily threat driven.

¹ European Commission, 'A Europe That Protects: EU Works to Build Resilience and Better Counter Hybrid Threats', Press Release, European Commission, 13 June 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123.

² Throughout this document, the term hybrid threats is used to cover a wide range of activities aimed at undermining the societal institutes, processes and coherence of a state, orchestrated and executed by another state actor, covertly and possibly indirectly through the use of non-state groups, so-called proxies. Note that the term denotes both potential (i.e. the threat of) and actual hybrid activities. Other terms with a similar meaning are variants on the 'hybrid' theme - hybrid conflict, hybrid warfare, hybrid campaigns, hybrid tactics, hybrid strategies - or on the notion of a 'grey zone' between peace and war in which the hybrid activities are executed.

2 TRENDS AND DEVELOPMENTS IN HYBRID CAMPAIGNS

2.1 GLOBALIZATION OF HYBRID THREATS

Hybrid conflict is spreading to new frontiers with smaller states acting as both the perpetrators and victims of hybrid tactics.

In 2014, the term hybrid warfare became part of the popular lexicon in relation to the conflict in Ukraine. A number of Russian hybrid campaigns against Europe have raised the concerns over hybrid tactics employed by revisionist states. But Russia is not the only actor utilizing hybrid tactics to gain a strategic advantage over other states. Across different regions in the world, states seem to be more able and willing to bypass international norms of non-interference. This is especially true in the information domain. As of 2019, at least seventy states had executed some form of (foreign or

domestic) disinformation campaign—a substantial increase from 2018 (48 states) and 2017 (28 states).³ Figure 1 shows which states had developed disinformation capabilities up to and including 2018, and which states developed disinformation capabilities during 2019.

Figure 1 shows that hybrid threats are not only experienced in the West, nor is it a strategy exclusively employed by great powers. In Asia, particularly China exercises hybrid influencing. An example is China's disinformation campaigns against Taiwan. In 2019, China shifted from utilizing domestic social media platforms to spread propaganda to using foreign platforms such as Facebook, Twitter and YouTube. Simultaneously, China is projecting influence through 'public diplomacy', which entails promoting Chinese language and culture worldwide through Confucius Institutes and shaping media to be pro-China.⁴

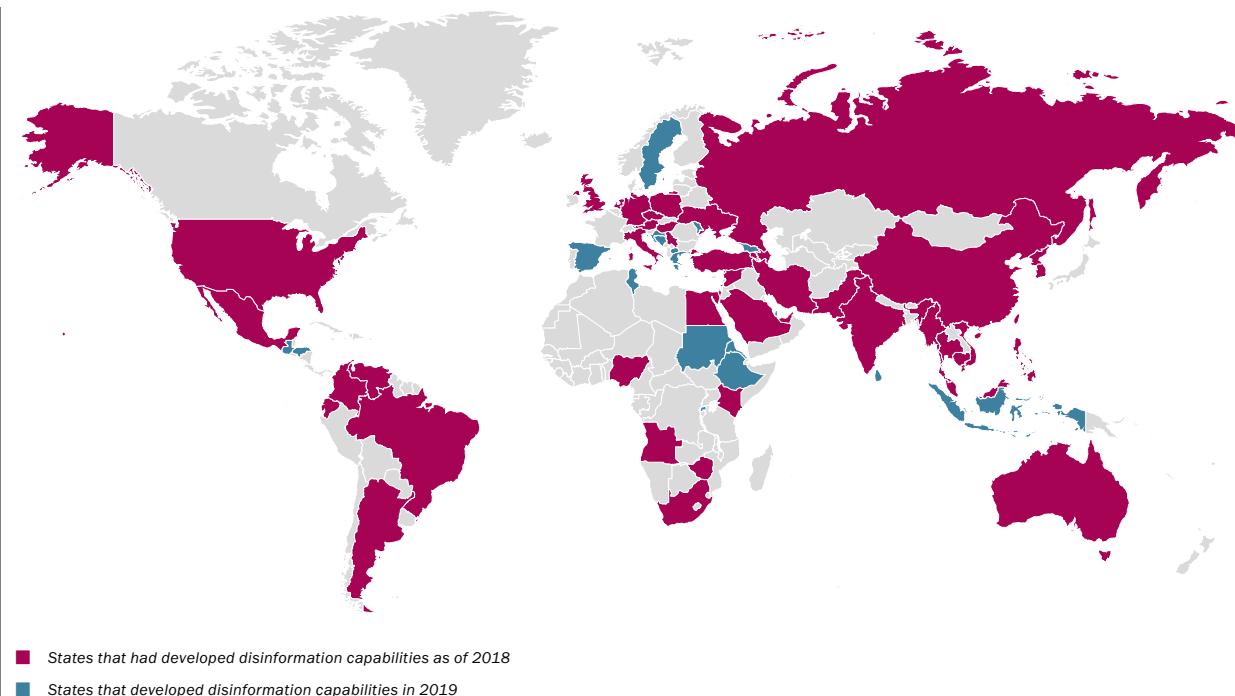


Figure 1: States that came onto the cyber-disinformation scene in 2019⁵

Iran's foray into cyberespionage

An example of the globalization of hybrid conflict is the activities of the Mabna Institute, a non-state, proxy actor linked to Iran. In February 2019, this group allegedly hacked into the Australian Parliament's computer system as part of their cyberespionage campaign to target members of FiveEyes, including the US, Canada, the UK, Australia and New Zealand. It is believed that the cyberattacks were a response to the Trump administration's withdrawal from the Iranian nuclear accord. Previously, the US indicted nine Iranian members of the Mabna group for stealing data from 320 universities in 22 countries, five federal and state government agencies, 47 private companies globally, and 2 non-government organizations.

³ Samantha Bradshaw and Philip Howard, 'The Global Disinformation Order: 2019 Global Inventory Of Organised Social Media Manipulation', Working Paper, Working Paper (Oxford, United Kingdom: Oxford Internet Institute, 2019), <https://comprop.oii.ox.ac.uk/research/cybertroops2019/>.

⁴ Public diplomacy is a process of 'government to people' communication through engagement with foreign publics, using words and deeds to shape public opinion. Such activities should be deemed hostile if they attempt to influence the population in a way that threatens to be hurtful to the target nation or undermines the ruling authority.

⁵ Data derived from; Bradshaw and Howard; Samantha Bradshaw and Philip Howard, 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation', Working Paper, Computational Propaganda Research Project (Oxford, United Kingdom: Oxford Internet Institute, 2018), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf>.

2.2 PRIVATE ROLES IN PUBLIC GOODS

The private sector is playing an increasing role in the realm of hybrid conflict – as a target and channel for spreading (dis)information; and as an entity capable of countering hybrid threats.

Private entities are emerging as prominent actors within the context of hybrid conflict in two ways. First, the public goods that private companies provide have made them a natural target for hybrid measures. Public social media platforms, mostly delivered by private companies, are now seen as critical for societies to exercise freedom of speech and freedom of assembly. The use of e.g. Twitter and Facebook as a medium for disinformation campaigns during elections have highlighted both the importance and the vulnerability of these platforms. This growing awareness has prompted several regulations on private companies and increased pressure on these companies to counter misuse themselves. This could be seen as shift from the multilateralist approach of the previous century to the multi-stakeholder approach that typifies the contemporary arena of international rules and norms; as well as a shift from a global laissez fair approach to a situation where smart regulation is sought.

Second, although attributing malicious behavior to particular sources typically remains the responsibility of states, the private sector has taken on an expanded role in attributing attacks, and has become instrumental in tracing cyber incidents, exposing malicious actors, and communicating this information to the public.⁶ Some private sector entities have launched efforts, such as the CyberPeace Institute, that are designed to monitor and expose large cyber events in a more systematic and extensive way. The idea of the private sector using its power and resources to hold actors accountable is

not a new one.⁷ In 1997, General Motors spurred the disinvestment of 125 foreign businesses from conducting business in South Africa during Apartheid, and more recently, many companies boycotted the Future Investment Initiative in response to the Saudi murder of Jamal Khashoggi.

Equation Group identified as a hacker group by a private actor

In 2015, Moscow-based Kaspersky Lab published a report in which the Equation Group was held responsible for infecting approximately five hundred systems in at least 42 countries. The malware used by the Equation Group had the ability to reprogram hard drives and then self-destruct, which made the operations effectively invisible and indestructible. Targeted systems ranged from private to public sector, and from military operations to media outlets.

The Equation Group is a highly sophisticated threat actor suspected of being tied to the Tailored Access Operations Unit of the US National Security Agency. Other companies, such as FireEye, CrowdStrike, Dell and Cisco have also taken the lead in investigating and attributing cyberattacks to the actor(s) responsible.

This discussion extends from the cyber domain to the information domain. For example, in December 2019, Reddit posted a statement declaring suspected meddling and disinformation from Russia on its platform and attributed the campaign to 61 Russia-linked accounts. Until recently, states possessed something close to a monopoly on attribution and therefore were able to control when, why, how and if the public was made aware of the information. This has and will further change. Although attribution is generally seen as a positive development, it may also complicate matters. Private actors may cause or exacerbate diplomatic disputes through attribu-

⁶ Sasha Romanosky and Benjamin Boudreaux, 'Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government', Working Paper, Working Paper (California, United States of America: RAND Corporation, 2019), https://www.rand.org/pubs/working_papers/WR1267.html.

⁷ Global Commission on the Stability of Cyberspace, "Advancing Cyberstability," November 2019



tion and reduce diplomatic or legal maneuvering space. There is further concern that states may pressure 'independent' private entities to assign blame to an adversary in order to stoke rivalries.

2.3 RISE OF LAWFARE

Lawfare is becoming a more eminent tool in hybrid warfare and leads to an increased disunity amongst states and distrust in the legal system and its guarding institutions.

Lawfare, also referred to as legal warfare, is defined as "the strategy of using or misusing the law as a substitute for traditional military means to achieve an operational goal."⁸ Lawfare also includes (ab)use of international legal and law enforcement agencies for national purposes. Lawfare as a hybrid tactic is on the rise. However, much like virtual all manifestations of hybrid threats, it is not a new phenomenon in itself.

Russia utilizes lawfare to influence the international system in pursuit of its national interests, even if it thereby also undermines the global order. Russian lawfare intertwines with and supports Russian information warfare, providing the (quasi-) legal justification of Russia's propaganda claims and aggressive actions. Russia's use of lawfare as a primary domain of its comprehensive hybrid warfare strategy poses structural challenges to the stability of the international security system and the foundations of the international legal order as a whole.

Examples of Russia's lawfare actions are: the use of the Western interventions in Kosovo and Libya as precedents for Russian interventions elsewhere; creating loopholes for OSCE-inspections for large scale military exercises by

reporting much lower numbers of military involved; and issuing a massive amount of passports for ethnic Russians in neighboring states.

Interpol weaponized through lawfare

An example of Russia's lawfare in full operation is through weaponizing Interpol, the leading international and intergovernmental police organization with 194 member states. The primary goal of the organization is to serve as an information hub in the fight against illegal transnational activities such as terrorism, drug trafficking, financial crimes, cyber hacks and human trafficking. Although Interpol cannot itself arrest or prosecute suspected criminals, it can facilitate national efforts to find and bring these individuals to justice. It does this mainly by so-called Red Notices and Diffusions (less formal than a Red Notice), which are international warnings that inform law enforcement authorities in the Member States that another country is pursuing the arrest of a specific person. National authorities can arrest and detain that person pending extradition to the complaining country. Despite rules designed to prevent their misuse, mechanisms like Red Notices and diffusions have increasingly become tools of repressive regimes. They call for Red Notices to repress dissidents against their own undemocratic regimes." With allegations of criminal or terrorist activity, the Kremlin and others abuse Interpol to extend their reach. Often, Russia uses ad hoc charges to brand people criminals and gain assistance from international law enforcement.⁹

Inevitably, other powers are following suit and resorting to lawfare tools to lay claims on contested areas (China in the South and East China Seas) or to justify their presence in volatile regions (Iran in various countries in the region, Turkey's involvement in Libya with claims on Mediterranean waters and resources in mind). The Middle East, Africa and Asia are particularly vulnerable to the application of lawfare, given the disputed nature of many state borders there. But NATO members are also not immune, especially those with sizeable Russian-speaking populations or with unresolved border disputes with Russia.

2.4 SPECIAL OPS OPERATIVES

Whilst focus mounts on new forms of hybrid conflict, the threat posed by more traditional hybrid tactics, such as assassination, remains omnipresent.

The 2018 assassination attempt of Sergei and Yulia Skripal, conducted by Russian so-called 'traveling special ops operatives', illustrates that assassinations, in flagrant contradiction with internationally agreed norms, are back on the table as a tactic. The threat of assassinations on European soil also stems from China and Iran.

In the Russian case, assassinations fit in a wider range of illegal activities on foreign soil. A recent example is the activities of Unit 29155, which has been associated with destabilization campaigns, poisonings, coups and assassinations in Moldova, Bulgaria, Montenegro and the UK. The activities of this Unit is of significant concern given the context of hybrid threats and increasing tensions between NATO and Russia, especially after the Skripal affair. The activities of Unit 29155 reflect transformational reforms to and significant operational bud-

get increases for Russia's military intelligence agencies since 2008.¹⁰

With the Skripal affair as a catalyst, concerns over the threat of 'domestic special ops operatives' in 'sleeper cells' in Europe and the US have also increased. Sleeper cells, small collections of spies who remain dormant in target societies until activated, are a traditional cornerstone of Russian (Soviet) military intelligence. Sleeper cells are also associated with Iran and with Iran-backed Hezbollah.

This kind of threat is problematic because over the past decades NATO countries have significantly downsized and underfunded their counterintelligence functions. Institutional knowledge and expertise to anticipate and prevent foreign 'special ops' in Western countries have diminished following the end of the Cold War and, particularly, after 9/11 when the 'war on terror' became the overriding priority. For the near future, Europe must become aware of the presence of these tactics, with the notion that Russia is probably not the only state to be pursuing the use of sleeper cells. In an age of technological leaps and bounds, the notion of a human as a valuable asset and serious threat must not be forgotten.

⁸ Charles Dunlap Jr., 'Lawfare Today: A Perspective', *Yale Journal of International Affairs*, no. Winter 2008 (1 January 2008): 1.

⁹ See e.g. Rasmus Wandall, Dan Suter, and Gabriela Ivan-Cucu, 'Misuse of Interpol's Red Notices and Impact on Human Rights - Recent Developments' (European Parliamentary Research Service, January 2019), [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU\(2019\)603472_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf).

¹⁰ As of 2016, this budget was said to be rising by 15-20% annually. Victor Madeira, 'Supplementary Written Evidence' (Parliament of the United Kingdom, 25 March 2016), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/31103.html#_ftn3.

Unit 29155: a dedicated unit for Russian hybrid operations

In October 2019, several media reports appeared about the existence of the ultra-secret Russian Unit 29155, which is carrying out hybrid actions to destabilize European countries. Intelligence officials from four Western countries concluded, according to these media reports, that the failed murder attempt on Russian former spy Sergei Skripal in Salisbury (UK) was part of a larger, well-coordinated Moscow campaign to destabilize Europe. Unit 29155 apparently has been active for at least ten years but was only recently discovered by the West. The work of Unit 29155, which falls under the military intelligence service GRO, aligns with President Putin's strategy to create what is called 'controlled chaos' in the West. In addition to the failed assassination attempt of the Skripals, Unit 29155 allegedly was responsible for a coup attempt in 2016 against the government of Montenegro. Western intelligence services then discovered the existence of the group for the first time. Two officers from the unit were involved in an attempt to overpower the government of Montenegro by assassinating the prime minister and seizing the parliament building.

2.5 MILITARY EXERCISES AS 'PSYCHOLOGICAL WARFARE'

Military exercises are treading a thin line between peacetime preparedness and provocation, increasing the chance of escalation.

Speeches yield importance not only from the words that they convey, but also from their context. The same is true of military exercises that occur near foreign borders. Military exercises have been increasing in size and scale over the last ten years, but their underlying intentions are more relevant. Ignoring the confidence building measures laid out by the Helsinki Act, some OSCE states continue to launch snap military exercises without notifying the international community. For example, in October 2019 the suspicion of forthcoming Turkish operations in North-Eastern Syria prompted Iran to conduct unannounced military exercises near the Turkish border. Earlier in the year, the potential of these exercises to kindle tensions was highlighted by the Iranian government when officials stated that US naval deployments near Iran were a part of "psychological warfare". Note that – fully in line with the ambiguous character of hybrid threats—this argument can also be reversed: the Iranian claim that US naval deployments are psychological warfare can itself be seen as PSY OPS, with a target audience that is both domestic and international.

Russia's claim about its new hypersonic weapon: real or 'psychological warfare'?

During his annual address to the Russian Parliament on March 1st 2018, President Putin openly proclaimed the development of new invincible missiles (the Avangard missiles) that were hypersonic and had an unlimited range. On 27th of December 2019 Russian Defense Minister Sergei Shoigu said in a conference call with Russian military leaders that the first missile unit equipped with the Avangard hypersonic glide vehicle entered combat duty. These claims were criticized by Western observers, stating that the Kremlin had signaled capabilities that it doesn't truly have in order to drive NATO to the negotiating table on terms favorable to Russia. Although performances might be overestimated, other experts believe that these weapons are in fact quite real and pose varying levels of strategic threat.

Threatening signals are also being portrayed through the unlawful incursion of military platforms entering the territories of other states. In the seas and skies, foreign aircraft and vessels are increasingly violating sovereign territory, leaving targeted states unsure how to react. In protest of Japan's ownership of three of the Senkaku Islands, China has been relentlessly intruding on Japan's contiguous zone since September 2012 (see Figure 2). The use of these practices appears to have increased, on par with a growing power competition. States are using exercises and intrusions as a provocative communication tool, creating distrust in the international order and fostering further tensions.

2.6 ECONOMIC STICKS, CARROTS AND SLEDGEHAMMERS

States are openly using economic measures for coercion and to exploit economic interdependencies.

Economic coercion is the employment of economic tools to exert targeted influence, and exploit vulnerabilities and interdependency relations for political purposes. Economically coercive tools include sanctions, manipulation of trade flows

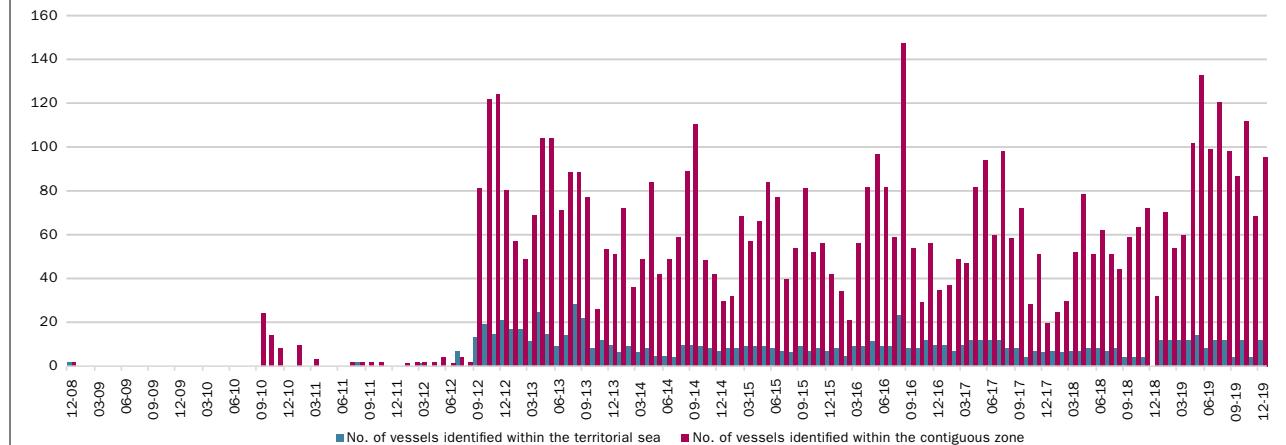


Figure 2: The numbers of Chinese government and other vessels that intruded Japan's contiguous zone into territorial sea surrounding the Senkaku Islands between December 2008 and December 2019 ¹¹

¹¹ Ministry of Foreign Affairs of Japan, 'Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response', Ministry of Foreign Affairs of Japan, 9 December 2019, https://www.mofa.go.jp/region/page23e_000021.html.



(including energy), and interdictions of goods and people. These tools are being increasingly utilized by states to maximize their power and influence abroad. As of the 11th of December 2019, the World Trade Organization (WTO) appellate body ceased to be operational due to expiring terms of two of its three judges who will not be succeeded by their nations. This serves as an indication that the norms of free trade underpinning the WTO are under threat.¹² Using economic coercion as tool for inflicting damage on a target state cannot be considered as a new tool for power projection, as it has been part of war planning, and of influencing throughout peacetime for decades. Recently, the trade war between US and China has created an environment whereby economic coercion is conducted openly and publicly. This overtness is unorthodox and challenges the status quo of the international system. When the US, once a beacon of free trade and liberal markets, employs economic measures to these ends and renders the dispute settlement body of the WTO toothless, other states are likely to follow suit. In the context of such developments, countries are becoming more open to utilizing economic coercive tools as hybrid tactics.

Russia banning direct flights from Russia to Georgia

The increasingly interconnected world feeds concerns over the weaponization of interdependence through the coercive use of asymmetric network structures. Russia's 2019 ban on direct flights to and from Georgia highlight how states can do this. In June 2019, in retaliation to anti-Russian protests in Georgia, Russia ordered a direct ban on all direct flights from Russia to Georgia, directly affecting tourism and business sectors, which are deeply dependent on flight route via Russia. There was no attempt made by Russia to mask the use of this tactic.

¹² Phil Hogan, 'Statement by Commissioner for Trade Phil Hogan on the Suspension of the Functioning of the WTO's Appellate Body' (European Commission, 10 December 2019), <https://trade.ec.europa.eu/doclib/press/index.cfm?id=2089>.

¹³ European Commission, 'Joint Statement by the European Union and Canada on an Interim Appeal Arbitration Arrangement', News Archive, 25 July 2019; Bryce Baschuk, 'China May Back EU's Trade-Dispute "Plan B" as Trump Hobbles WTO', Bloomberg.Com, 10 December 2019, sec. Economics, <https://www.bloomberg.com/news/articles/2019-12-10/china-may-back-eu-s-trade-dispute-plan-b-as-trump-hobbles-wto>.

We can expect these tactics to be used more frequently, especially in the absence of a regulating body. The EU has put forward an alternative regulating body, but the absence of important players, such as the US, creates doubt in this plan.¹³ Nonetheless, there is a clear need for Von Der Leyen's Commission to push for a solution in the regulation of trade and economic disputes. If not, lacking a united front to withstand pressure, EU member states run the risk of being significantly affected by an increase of economic coercion in the coming years, and subsequently losing influence in the international arena.

2.7 HIDING BEHIND PROXIES

Proxy actors are increasingly used by states to engage in conflict whilst avoiding direct culpability.

If states wish to influence and engage in armed conflict, but hope to distance themselves from the consequences, they may employ proxy actors as a shield against attributions. Intelligence and security services have historically infiltrated private groups; note the activities of football hooligan paramilitaries in the Yugoslavian wars and the use of proxy forces by the US in the Middle East since 2001. However, the increased sophistication of the use of these groups and their capabilities does present a sense of novelty.

Recent examples of proxy activities show complex patterns of dependency between state and non-state actors. In Ukraine, Russia uses criminal gangs to destabilize the political domain. In Taiwan, criminal groups with links to China have been engaged to aggravate pro-democracy protests. The Wagner group, a private military company operated by the Kremlin has been spotted in several countries, such as Ukraine, Syria, Sudan,

the Central African Republic and Libya. An example of the group's work can be seen in Sudan, where they are being employed to share know-how to pro-regime forces, as well as to guard mines of Russian companies, such as M-invest.

Iran's "Axis of Resistance"

Iran's loose confederation of like-minded state and non-state actors across the Middle East to counter Western influence is often referred to as the Axis of Resistance. These partners, proxies and allies include the Assad regime in Syria, Hezbollah in Lebanon, Shia militias in Iraq, the Houthis in Yemen, Bahraini militants, and some Palestinian groups. There even have been attempts to integrate the Shia militias in Iraq, fighting under the banner of the Popular Mobilization Forces (PMF), into the regular Iraqi Forces, until now without success. Most of these proxies are Shia entities (see Figure 3) but select Sunni groups—like HAMAS—also align with Iran on key issues. The axis helps Tehran extend its influence in the region by putting pressure on non-friendly nations through support (e.g. weapon deliveries, combat training) of these partners.

Proxies are also employed for gaining influence with the potential to exploit this influence when needed in the (near) future. China's state-owned (or supported) enterprises involved in building, funding and/or operating maritime ports in Asia, Africa and Europe may be used for leverage by China. Chinese port operations or ownership pose immediate risks to Western interests, potentially allowing China to extract intelligence, to block e.g. NATO vessels from accessing services (e.g. at Djibouti), and to use ports to dock military vessels. More subtly, economic and financial dependencies can be turned into political influence. For example, in Israel, China is building two new ports, in Haifa and Ashdod. Local academics as well as US pressure have urged the Israeli government to assess how much China can be involved in its economy without compromising its security interests.

Looking forward, private companies are emerging as actors capable of employing hybrid threats under government pressure.¹⁴ An example of such pressure was illustrated in the role played by the SWIFT financial messaging service in US economic coercion against Iran. Moreover, there seems to be a transfer of knowledge between countries through companies. This was seen in Sudan, where a Russian company, M-Invest, acted as an advisor for suppressing protests against the Sudanese regime. For the future, the role of private companies as actors, either it is as an actual perpetrator or an actor forced to act in a government's favor, cannot be ruled out or should even be expected, as no longer private businesses, regardless of industry, are isolated with national security.

Education institutes as vehicles for proxy actors

Educational institutes may be used by proxy actors as part of the hybrid toolbox. The number of Chinese students studying abroad reached 662,100 in 2018, up 8.8% from a year earlier. The number of overseas students returning home after graduation totaled 519,400 in 2018, 8% more than the previous year. There are concerns that Chinese university students in the United States and other Western states are being pressured to conduct acts of espionage. Meanwhile, Chinese students abroad and academic organizations are used to spread the Party's narrative on e.g. Tibet and the Dalai Lama. In June 2019, the Dutch media program Nieuwsuur reported that China can educate military scientists in the Netherlands without oversight or interference from the Dutch government. Based on public sources, Nieuwsuur compiled a list of more than twenty Chinese scientists who graduated from the National University of Defence Technology in China before joining the PhD program at Delft Technical University. Their studies typically involved dual-use technologies that could well be used for military purposes, such as models of war simulations and algorithms for analyzing and influencing social media users. Neither the government nor TU Delft actively supervised this.



Figure 3: China's Belt and Road Initiative, displaying existing and planned ports in Asia, Africa and Europe through which China can exert influence.¹⁵

¹⁴ Bianca Torossian, Tara Görder, and Lucas Fagliano, 'Hybrid Conflict: Neither War, nor Peace', Strategic Monitor 2019-2020 (The Hague, Netherlands: The Hague Centre For Strategic Studies, 10 January 2020), <https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/>

¹⁵ <https://www.dw.com/en/china-a-loan-shark-or-the-good-samaritan/a-48671742>

2.8 POLITICAL MACHINATIONS

States meddle in other countries' internal political affairs through election interference and the financing and influencing of political parties and civil society actors.

Following the Brexit referendum in the UK and the 2016 US Presidential election, discussion over election interference and political interference by foreign countries became widespread. In both cases, the complex and multidimensional nature of political interference was revealed, as the 'attack' was not executed through a single disinformation campaign or cyberattack. Instead, a comprehensive campaign that combined lobbying, disinformation, corruption and cyberattacks was carried out.¹⁶ Some observers note that, even without possible external interference, some political campaigns are already riddled with dubious, if not outright false, information. This makes the life of hybrid actors easier; they only inflate what is already there.

Whilst, again, there is nothing inherently new about states interfering with the political affairs of another state, social media and technological developments that enable and encourage the mass dispersion of information means that actors can influence public life in foreign states with greater ease than ever before. Over the last four years, Europe has been consistently targeted with political interference campaigns, including during the Catalan Independence Referendum, the French presidential elections, the EU Parliamentary elections and the Austrian elections. The financing of religious organizations (e.g. of Koran schools and Mosques) could also be a part of such campaigns. The more comprehensive such campaigns, the less effective counter-

measures that treat each domain or tool as a stand-alone arm. This trend is being progressively recognized by EU member states, as the threat posed by influencing and political interference are becoming codified in strategic foresight and security documents.¹⁷

Foreign influence in Latin America

In Latin America, protests in October and November of 2019 in Bolivia and Chile showed signs of foreign interference. Venezuelan operatives inside Bolivia were reported to be inciting and participating in violent protests against the new Bolivian government. This tactic of agitation was complemented by divisive information campaigns through Russian-owned media outlets RT and Sputnik.

2.9 SHIFTING REALITIES

Spurred on by technological advancements, disinformation and fake news campaigns are growing in occurrence, scope and impact.

Disinformation is an evolving phenomenon. While today bots are a matter of concern, it is virtual impersonation and social dialogue distortions that will emerge as key threats over the next few years. States are increasingly utilizing digital disinformation capabilities to influence, interfere with, and disrupt other states. In Europe, reports claimed Russian influence during the Catalan referendum was employed to seed discontent through the creation of misleading content, in combination with amplification through bots.

Whilst bots are still relevant, new technologies have emerged on the horizon and are expected to have a disruptive impact on disinformation technologies. At the core of this concern are deepfakes. Produced by deep-learning algorithms, deepfakes are highly realistic and difficult-to-detect depictions of real people doing or saying things they never said or did. Whilst the use of this technology is still experimental and does require a level of technological sophistication, deepfakes are poised to change the disinformation game. Fake videos that are created with simpler editing tools (referred to as 'cheapfakes') can also have detrimental impacts on information domain.

Cheapfakes are already on the mainstream scene. In 2019, US President Trump shared a cheapfake video of Nancy Pelosi, speaker of the US house of representatives, appearing to give a speech whilst inebriated. Commercial apps which attempt to produce lip-synced or AI-based doctoring are already on the market and can be used by anyone to manipulate content. In Gabon, after months of uncertainty over Gabon's president health, the release of a potential deepfake was enough to instigate a coup d'état. This example shows how deepfakes can exacerbate fragile conditions and cause confusion and chaos.

Certain asymmetries are coming to light in the arena of media and information as states are able to exploit democratic values through information warfare whilst protecting themselves through control and surveillance. How to regulate disinformation in a period where deepfakes and cheapfakes are being doctored and distributed will be especially challenging for societies that value freedom of speech and freedom of expression. Indeed, Facebook notoriously refused to remove the cheapfake video of Pelosi, given that the content did not violate the company's 'community standards.

Just as deepfakes convey disinformation through the senses of sight and sound, the coming years could see virtual reality used for multisensory propaganda experience. Advancements in AI, virtual reality, augmented reality and machine learning will change the way we interact with the news and information. In a world where societal cleavages are on the rise, narrative is a powerful tool to wield. Without regulation and societal resilience, advanced technologies can change our understanding of the 'battlefield'.¹⁸

With the rise of the Internet of Things and algorithmic, big data-driven processes, advanced societies are becoming perilously dependent on networks of information and data gathering and exchange for communication, analysis and decision-making purposes. Aggressors will increasingly have the opportunity, not merely to spread disinformation or favorable narratives or to damage physical infrastructure, but to skew and damage the functioning of the massive databases, algorithms and networks of computerized devices on which modern societies utterly depend. A shift from front-end manipulation (messages, narratives, stories etc.) to back-end manipulation (data, algorithms, networks etc.) will occur. In a recent RAND study this phenomenon is described as 'virtual societal warfare'.¹⁹ The primary goal of virtual societal warfare is creating confusion and an accelerating loss of confidence in the operation of major social institutions. Attacks on the effective operation of information systems undermine social trust in the institutions and processes of advanced societies and might generate a sense of persistent insecurity and anxiety.

¹⁶ For an analysis on political interference campaigns, see Robert Mueller, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election' (Washington D.C., USA: U.S. Department of Justice, March 2019), <https://www.justice.gov/storage/report.pdf>.

¹⁷ Hugo Van Manen, Lucas Fagliano, and Marek Baron, 'In the Eye of the Beholder? An Assessment of Global Security Perceptions', Strategic Monitor 2019-2020 (The Hague, Netherlands: The Hague Centre for Strategic Studies, 14 January 2020), <https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/in-the-eye-of-the-beholder/>.

¹⁸ Peter Singer and Emerson Brooking, 'What Clausewitz Can Teach Us About War on Social Media', Magazine, Foreign Affairs, 4 October 2018, <https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media>.

¹⁹ Michael J. Mazarr, 'The Emerging Risk of Virtual Societal Warfare', Research Reports (California, United States of America: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html

2.10 FORMATION OF DIGITAL ISLANDS

National sovereignty pushes the demand for national governance of the internet, to some extent even for a national internet, making it easier to threaten or attack other's internet infrastructure.

Russian and Chinese efforts towards a national internet is driven by the doctrine of internet sovereignty, or the right of states to govern the internet in line with its domestic laws. These laws, which were originally applied to traditional media forms, became equally applicable to content online. Introducing national segments of the global internet has two security consequences. First, such a national internet is more difficult to attack. Second, a cyberattack launched from such an internet is more difficult to attribute and counter. As a result, having a national internet makes it easier to threaten or attack other's internet infrastructure because attribution and retaliation is made more difficult.

This development is not confined to Russia and China. As the most recent Freedom on the Net report purports, "as governments recognize the importance of the data flowing in and out of their countries, they are establishing new rules and barriers in the name of national sovereignty, allowing officials to control and inspect such information at will."²⁰ This said, it would be a mistake to exclusively link internet sovereignty to authoritarian regimes. The same underlying principles affect Western governments. Governing which aspects of the web are available to users has been the de facto position of governments worldwide since at least the late 1990s. Any government might be worried about malicious information like malware reaching military installations and critical water and power grids, or fake news influencing the electorate. In the U.K., for example, there are currently plans to introduce an age-verification system for adult content.

Russia testing disconnection from the worldwide internet

In December 2019, Russia ran a series of tests to disconnect the country from the worldwide internet, involving Russian government agencies, local internet service providers, and local Russian internet companies. The goal was to test if the country's national internet infrastructure, known as RuNet, could function without access to the global domain name (DNS) system and the external internet. The experiment was deemed a success, according to the government. Internet traffic was re-routed internally, effectively making Russia's RuNet the world's largest intranet. Up to a point, RuNet is modelled after the Great Firewall of China, a combination of legislative actions and technologies enforced by the People's Republic of China to regulate the Internet domestically. It blocks access to selected foreign websites and slows down cross-border internet traffic.

With the possible exceptions of North Korea and Iran, Russia's ambitions exceed those of other states, and accordingly, the recent RuNet tests are a culmination of multiple years of planning, law-making, and physical modifications to Russia's local internet infrastructure. Its new methods raise the possibility not only of countries pulling up their own drawbridges, but of alliances between like-minded countries to establish a parallel internet, effectively fracturing the global internet and leading to so-called digital islands.

However, Russia's neighbors, like the Central Asian Republics, could leverage Russia's architecture, to connect only to the RuNet version of the Internet. Countries entangled in the Chinese Belt and Road Initiative might prefer an infrastructure built around China, allowing them to participate in a semi-global economy while being able to control certain aspects of their populations' internet behavior. Large countries like Brazil

and India may adapt the technology to create an intermediate position that relies neither on 'open values' nor on closed national intranets. In short, "whether the information borders are drawn up by individual countries, coalitions, or global internet platforms, one thing is clear – the open internet that its early creators had in mind is already gone."²¹

2.11 CYBERSPACE: THE FRAGILE UNDERBELLY OF SOCIETY

Cyberattacks are growing in occurrence and caused damage and are likely to become a defining element of hybrid conflicts.

Few threats are more closely associated with hybrid warfare than cyberattacks. Targeting critical infrastructure from a distance through cyberspace constitutes an attractive method for undermining states. Continuous reconnaissance and cyberattacks on critical infrastructure are increasing. In the absence of comprehensive rules and regulations, or even agreed-upon regulatory frameworks, at the international level, this domain remains a risk for the international system. Examples of this can be seen in the attacks of WannaCry, which spread ransomware to 300,000 computers in 150 countries, creating massive disruptions for businesses and critical infrastructure, such as hospitals. Against a backdrop of Russian-US tensions, the US has begun attempting cyberattacks in Russian energy grids. These attacks are symptomatic of a growing trend toward the strategic targeting of critical sectors.²²

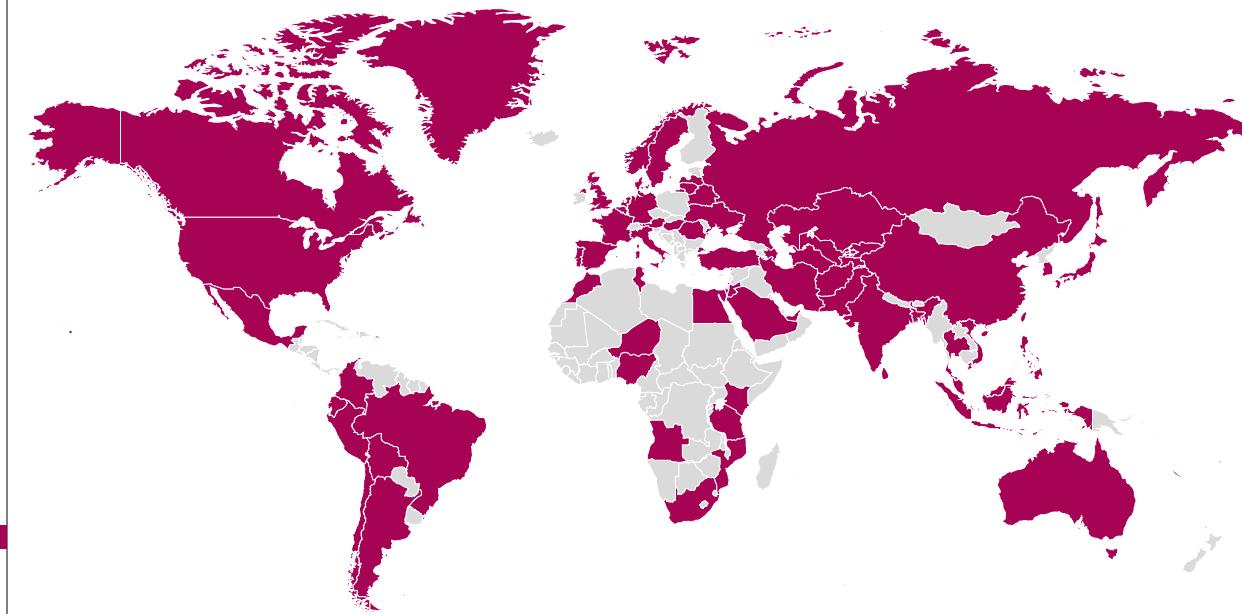


Figure 4: Countries initially affected in WannaCry ransomware attack²³

21. Sally Adee, 'The Global Internet Is Disintegrating. What Comes Next?', BBC, 15 May 2019, In Depth edition, sec. Future, <https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next>.

22. Tania Latici, 'Cyber: How Big Is the Threat?' (Brussels, Belgium: European Parliamentary Research Service, July 2019), 1, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA\(2019\)637980_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf).

23. Wikimedia Commons, 14 May 2017

20. See Adrian Shahbaz, 'Freedom of the Net 2018: The Rise of Digital Authoritarianism' (Washington, D.C.: Freedom House, October 2018), https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

Considering modern society's increasing dependence on the internet (and cyberspace more broadly), new opportunities for cyberattacks are arising. The digitization of our societies—from the digitization of citizens' identity documents to the automation of everyday infrastructure such as 'smart doors'—mean that malicious actors have ever-increasing systems to target for ransom, espionage, disruption and hacking. As interstate military competition increases, more cyberattacks are expected to be carried out by states, though the covert nature of cyberattacks and the use of proxy actors makes attribution challenging. As mentioned in section 2.10, the development of national internets, such as RuNet, pose an additional threat as cyberattacks may be executed more effectively whilst attribution will be avoided.

Triton malware could have led to many casualties

In 2017, a piece of malware called Triton infected systems of a petrochemical plant in Saudi Arabia. What made Triton different from other malware was that the code was aimed at manipulating essential factory security systems. These security systems are the last line of defense and can stop operations when dangerous conditions are detected by sensors or warning systems. Triton offered the attackers the ability to successfully access the security systems remotely. Fortunately, however, due to an error in the malware, it was rendered harmless once detected. According to security experts, a successful attack could have caused an explosion and thereby, endangered human lives. Even though Triton was discovered in time, companies specializing in industrial security are seeing new variants of this malware appear. Moreover, these variants are not only signaled in the Middle East, but also in other parts of the world.

2.12 EMERGING TECHNOLOGIES: AMOUNTING TO NEW CAPABILITIES

Emerging technologies like Artificial Intelligence (AI) and Internet-of-Things (IoT) amount to new capabilities, holding the potential to intensify and revolutionize hybrid conflict.

The conjunction of new technologies and hybrid tactics will continue to present unique opportunities and challenges. Authoritarian regimes are increasingly becoming aware of the potential of AI and the IoT as a means to monitor and manipulate citizens. The impact of these technologies will be felt, not only in states where rule of law and democracy have not been fully institutionalized, but also in rule-based societies. Given the increased presence of AI and IoT in everyday appliances, there is increased possibility that states will use AI to gather information on target audiences and opposing forces in order to engage in 'cognitive hacking'.

The private sector is the driving force behind many of the emerging technologies. Intelligent virtual assistants such as Alexa have proven vulnerable to be converted into spying devices. Hence, the role of a company like Amazon may become that of an espionage middleman. Moreover, with the increasing breadth of the IoT, "Do-It-Yourself" attacks are becoming more feasible and attractive to malicious actors. Basic infrastructure such as traffic lights, road signs and automated cars, can be already hacked to generate unprecedented disruptions. The upcoming technologies associated with smart cities, or alternative sources of energies, which require connection to 5G networks and other devices, could entail further weaknesses. The controversy over Huawei's 5G networks portrays further participation of private-driven technological developments as part of power competition and hybrid strategies. Overcoming these vulnerabilities will challenge the boundaries between law enforcement and the military. To this regard, the role of all new and emerging technologies, not only those such as AI-based missiles, but also

common apps and devices which are part of the nebulous of IoT, must be examined.

In the next chapter we will provide an overview of the most relevant emerging technologies in the context of hybrid threats.





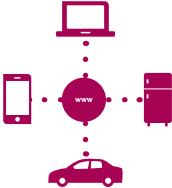
3 EMERGING TECHNOLOGIES AND CAPABILITIES IN HYBRID THREATS

3.1 THE WHY AND WHAT OF EMERGING TECHNOLOGIES

Developments in science and technology have the potential to transform the character of warfare and conflict. Most major innovations no longer originate from government-controlled military laboratories, but from commercial markets. Due to the nature of hybrid threats, which span multiple domains including the military, the economic and the information domains, the list of potentially relevant technologies is large.

The table below depicts a set of technological developments (and in some cases capabilities in which multiple technologies will be combined) relevant for the evolution of hybrid threats. This set reflects notable developments that have taken place in recent years. Most of the emphasis is given to technologies and capabilities in the virtual and information domain, since this is where both state and non-state actors can act quite freely without being caught in an act of war. In the next sections, these technologies are elaborated on in more detail.

Emerging Technologies...	... and their implications for hybrid conflict	
	<p>Additive manufacturing</p>	<p>The ability for rapid, decentralized and flexible production of systems makes additive manufacturing attractive and easy to use for terrorist and/or non-state actors (e.g. for building and employing drones equipped with munitions or CB-agents). Designing, prototyping and building a drone is a traditionally challenging task, requiring days or weeks of research and development, design, construction and testing before the drone is ready to take flight. Additive manufacturing (or 3D printing) gives businesses and consumers the tools to create their own drones in a matter of days. Similar considerations apply to various other devices that can be used maliciously.</p>

Emerging Technologies...	... and their implications for hybrid conflict	
	Unmanned and Autonomous Systems	Unmanned systems are omnipresent in our daily lives. Technologies like AI, deep learning and big data accompany the development toward greater autonomy for unmanned systems. Using AI for navigation and identification enables these systems to have an advanced degree of autonomy. With these capabilities the attribution of, and responsibility for, autonomous systems are somewhat unclear. However, as these systems have the potential to move humans out of danger zones, they are likely to be used as weaponry.
	Extended and Synthetic Reality	Bots with advanced AI capabilities will resemble human beings (physically and visually) on social media platforms, thereby creating a synthetic world. Whilst we are currently reacting to the presence of deepfakes, bots will also appear in our physical world, leading to Extended Reality spaces (as used in gaming, simulations and training). This synthetic world will be created with such high quality that the distinction between real beings and computer-generated beings (such as avatars and holograms) will be less clear, providing malicious actors with a tool for a more advanced manipulation of reality.
	Internet of Things (IoT)	The emergence of an IoT carries enormous potential for both classic cyberaggression and social manipulation. Everything is becoming one complex hyperconnected system. Even if things do not interoperate, they exist on the same network and affect each other, causing cascading effects once one system is hacked or misused. Currently, 26 billion connected devices are installed worldwide. This number will grow exponentially in the coming years, with predictions set to amount to 75 billion by 2025. However, it is not just the interconnectedness between systems, but also the way in which they are integrated into everyday life, that will create implications for hybrid conflict.

Emerging Technologies...	... and their implications for hybrid conflict	
	5G network technology	5G, the fifth generation of cellular network technology, supports high-speed telecommunications, which improves not only speed, but also latency, power consumption and capacity (bandwidth). 5G networks therefore enable the use of computer-intensive new technologies that require bandwidth and fast computer power, such as Artificial Intelligence and deep fakes that can be used to manipulate information and media. 5G is also the enabler for the explosive growth of the Internet-of-Things. With Huawei currently offering 5G to many countries, the 5G race is on.
	Satellite jamming, spoofing and hacking	A disruption of satellite navigation or communications systems can have serious consequences for society. In future conflicts, we might expect targeting of satellites, e.g. by hacking, jamming or spoofing, or even neutralizing them by space-based laser or missile weapons. The trend of miniaturizing satellites, and the involvement of commercial parties in launching these satellites, have given a wider audience access to this domain, which comes with associated dangers.
	Offensive cyber tools	The evolution of cyber warfare and its tools is progressing. New phenomena like co-option of hacking tools and bypassing two-factor authentication have just emerged and will quickly gain popularity. The co-option of hacking tools by third parties, makes attribution challenging and enables the creation of new sophisticated cyber tools through learning and adapting from other tools used previously. Another recent advancement in is the bypassing of two-factor authentication (2FA), which gives hackers access to government entities and managed service providers active in fields like aviation, healthcare, finance, insurance, energy, and even in niche areas such as gambling.
	Micro or finetuned targeting	New technologies like neurohacking will enable much more consistent and targeted isolation of specific individuals with highly customized messages. Additionally, kinetic means, such as the integrated combination of social media (to profile people), extensive networks of sensors and lethal micro drones (insect-sized), can be used to neutralize targets at the right time and place without risking attribution and collateral damage.

3.2 ADDITIVE MANUFACTURING

The potential for rapid, decentralized and flexible production of systems makes additive manufacturing attractive and easy to use for terrorists and other non-state actors.

Additive manufacturing (or 3D-printing) provides the ability to manufacture on demand and on location. The concept of additive manufacturing houses a range of different technologies, all sharing the concept of “layer by layer” manufacturing, whilst each having different characteristics in terms of materials, technical capabilities, constraints, etc. Products can be manufactured in a decentralized manner, which will alter current supply chains. The transport of end-products will make way to the transport of design data and raw materials. The military’s logistic footprint may be significantly reduced whilst readiness and maneuvering capabilities will be enhanced. Other potential advantages in this context include lighter weight products, multi-material products, ergonomic products, efficient short production runs, fewer assembly errors (and therefore lower associated costs), lower tool investment costs, the combination of different manufacturing processes, optimized material-use, and more sustainable manufacturing processes.

The downside, of course, is the potential for misuse by terrorists and criminals. Constructing a drone, for example, is normally a challenging task that requires lengthy periods of research and development, design, construction and testing. 3D-printing gives businesses as well as consumers the tools to create their own drones in a matter of days.

Traditionally, non-state actors with military capabilities, (such as ISIS, Hezbollah and the former IRA), are effective at launching hybrid tactics, but generally lack the logistical means that typify conventional armed forces, making the sustainability of operations difficult (Hezbollah being an exception). With additive manufacturing they may reduce that disadvantage.

3D (partly) printed weapon used in the Halle synagogue shooting

On the 9th of October 2019 in Halle (Germany), a shooting in a synagogue took place. After unsuccessfully trying to enter the synagogue in Halle during Yom Kippur, the attacker killed two people nearby and later injured two others. He allegedly used steel, wood and 3D printed plastic components to manufacture a 9mm submachine gun, a 12-gauge shotgun and a pistol. The International Centre for the Study of Radicalisation (ICSR), commented that although the attacker constructed several weapons that involved 3D printing, none of these weapons were entirely 3D printed. Nonetheless, the event represents a first instance of things to come. As 3D-printing develops, the weapons it can produce become deadlier and harder to trace, it will ease cross border weapon transport, and will likely yield a new industry of homemade weaponry disseminated online.

The technology will give terrorists easier access to a spectrum of increasingly dangerous weapons, and new ways to evade government countermeasures. Unlike conventional firearms, 3D printed guns have no serial numbers, hindering government efforts to track their origin, sale and ownership. They can be easily disguised to deceive the untrained eye and appear as something more innocuous, and because they are made of plastic, they are invisible to metal detectors. The 3D printing of weapons for acts of terrorism will probably extend beyond firearms to other weapons like drones and bombs.

3.3 UNMANNED AND AUTONOMOUS SYSTEMS

The attribution and ownership of unmanned and autonomous systems is difficult to determine, making these systems attractive for covert operations.

Unmanned systems are omnipresent in our daily lives. They operate on land, at sea, in the air and in space, in a variety of application domains such as traffic, health care, logistics, military, industrial processes and energy. Currently, their degree of autonomy is limited, and in most cases the human is still “in the loop”, controlling or monitoring the unmanned system. The use of the term ‘autonomous system’ is therefore not always consistent with the system’s actual degree of autonomy. However, due to rapid advancements in AI, sensors and ICT (computing power, communication latency and speed), the transition from semi-autonomous systems to (near-to) fully autonomous systems will take place. The speed of this transition will vary with the application domain, due to differences in regulations, governance, safety and security risks.

The commercial drone market is expected to grow to 43 billion US dollars worldwide by 2024, three times the market size of 2018.²⁴ Advancing technologies will make it possible to equip drones with high performance sensors and other payloads (including e.g. explosives), allowing them to be used for longer ranges and in a more autonomous mode. This provides actors (states, non-state actors and skilled amateurs) with the option to use these drones for spying, tracking and engaging persons, and damaging vital infrastructure. Because operators remain at distance, attributing the use of drones to specific persons or organizations will become more difficult. This will ease the malicious use of drones for criminal and terrorist activities, possibly as part of a larger hybrid operation or campaign.

Drone attacks in Arabian Sea as part of hybrid warfare

The 2019 incidents in the Arabian Sea showed how drones may be used covertly as part of hybrid warfare operations, without attribution. The 14 September 2019 drone attacks on Saudi Arabian oil plants, probably executed by Iran or Yemen, caused so much damage to Saudi Arabia’s oil facilities of Aramco that its production was cut by 50%. Analysis of satellite images of the Aramco facility before and after the attacks appear to show nineteen individual strikes: fourteen that punctured storage tanks, three that disabled oil processing trains, and two more that damaged no equipment at all. Although the UN carried out a thorough investigation about the origin of the drone attack, it stated in December 2019 that its investigation was not able to confirm the Saudi official claim that the weapons used in the attack are of Iranian origin.

The use of unmanned systems for hybrid operations is not restricted to the air domain (drones) but also covers the land and sea domains. A few days after the drone attacks on Aramco, the Saudi armed forces stated that they intercepted and destroyed an unmanned explosives-laden boat launched from Yemen by the Iran-aligned Houthi group. Since 2017, there have been several reports of attacks or discovery of these unmanned explosive boats in the country.

With the growing development of autonomy for unmanned systems, swarming concepts will become more intelligent and capable. Swarms of unmanned systems are defined as interconnected intelligent systems that can work together to accomplish one or more tasks. During the opening ceremony of the 2018 Winter Olympics, a foreshadowing of the potential

²⁴ Lukas Schroth, ‘The Drone Market 2019-2024: 5 Things to Know - DRONEII.Com’, Drone Industry Insights (blog), 10 April 2019, <https://www.droneii.com/the-drone-market-2019-2024-5-things-you-need-to-know>.



Figure 5: At the 2018 Winter Olympics, over 1200 specially designed drones were illuminated and danced in the sky, forming, among other images, a giant snowboarder and the iconic five rings of the Olympics.²⁵

of swarming drones was provided when over 1200 specially designed drones gave spectators a unique visual show. An entire drone swarm, properly programmed, can be controlled by one operator, with flights generally lasting five to eight minutes. Whilst the spectacle shown at the 2018 Winter Olympics was innocuous and entertaining, the imagination does not have to stretch far to predict that such synchronized swarms could be used for malicious means.

Another relevant development is the stealth drone. Stealth drones (mostly medium and large sized drone classes) are less detectable for radar systems and can be used for covert intelligence and surveillance operations, a crucial element in hybrid operations. This development is progressing rapidly, and China appears to be currently leading the game. During the military parade held as part of China's celebrations for 70 years of Communist Party rule, the stealthy DR-8 drone attracted much attention, particularly due to its sleek shape and supersonic speed.

3.4 EXTENDED AND SYNTHETIC REALITY

Extended and Synthetic Reality will shape new environments that are more difficult to distinguish from reality and are therefore an attractive technology for manipulating perceptions.

Extended reality (XR) is a term referring to all real and virtual combined environments and human-machine interactions generated by computer technology and wearables. It includes representative forms such as augmented reality (AR: a real-world environment where objects that reside in the real world are enhanced by computer-generated information), mixed reality (MR: a merged environment of real and virtual worlds to produce new environments and visualizations) and virtual reality (VR: a computer-generated simulation that can be interacted within a seemingly real or physical way by a person) and

the areas interpolated among them. The overall goal of these Extended Reality environments is to present digital content that informs and/or interacts with our senses as naturally as possible in order to achieve an immersive experience that leads to better planning, decision-making, training or execution of processes or tasks in daily life, both for pleasure and for working.

Over time, high-end computer-generated imagery (CGI) and similar technologies (audio, interfaces) will penetrate consumer markets, allowing for widespread use of hyper realistic computer-generated imaging and video production by private companies and individuals. A recent PricewaterhouseCoopers study suggested that VR technology is on the verge of an explosive uptake, projecting that there will be over 55 million VR headsets in active use in the United States by 2022.

Although XR offers a lot of potential advantages for personal and working environments, it also poses some new threats that align with misleading and deception activities, which can be part of a hybrid campaign. Studies warn that emerging XR systems could be vulnerable to hacks. Hackers could insert additional details into XR environments designed to create stress or skew results. These actors could find ways to send messages subliminally, seeding users with certain views or disruptions. Broadly speaking, XR offers whole virtual worlds that manipulators can hack and modify to achieve their desired goals.

In addition to Extended Reality, we also face Synthetic Reality (SR) technology, such as deepfakes, which fall under the wider category of AI-generated 'synthetic media'. This is audiovisual information in digital form which is a composite of multiple synthesized information pieces in order to produce a new informational artefact or (faked) reality. When Extended Reality (AR/VR/MR) and Synthetic Reality (such as video and audio fakes) meet and operate symbiotically, they reinforce each other's perceived levels of realism. Examples of the use of this combination for malicious activities may be just a few years away. Today, immersive technologies are applied primarily in games, but within the next twenty years, it is predicted

that these technologies will be as much in use as smartphones are today. In the medium-to-long term, bots with advanced AI capabilities will resemble human beings (physically and visually) on social media platforms and in XR spaces well enough that we will not be able to distinguish real from CGI beings.

Audio deepfakes

In September 2019, media outlets reported that audio deepfakes were applied by criminals to trick a UK energy company manager into wrongly transferring €200,000 to a purported supplier in Hungary. The perpetrators were likely part of an organized crime group. A deepfake was used to imitate the sound of the manager's boss' voice, and not only the voice but also the tonality, the punctuation and the accent. When the fake voice requested the payment be made, the manager complied.

One step further in future, we may see holograms entering the hybrid battlefield. Pentagon researchers have repeatedly suggested the use of large lifelike holograms above the battlefield, for example the use of a spaceship hologram to intimidate people on the ground, or the use of multiple holograms of tanks escorting one or two real tanks, faking a complete tank platoon. One might even imagine a very realistic hologram of a key leader speaking to a diaspora in a foreign country. Such holographic technology is already being developed in the movie and entertainment industry. Improvements are, however, still needed, particularly with regard to moving holograms. In 2010, when researchers from the University of Arizona carried out experiments with moving holograms, these movements were still very erratic and unsynchronized, but demonstrated potential. With improved image and calculation algorithms being developed, the issues with time lag will soon be solved, and gradual movement of holograms will be possible.

²⁵ 'Intel Drone Light Show Breaks Guinness World Records Title at Olympic Winter Games PyeongChang 2018', News Release, Intel Newsroom (blog), 9 February 2018, <https://newsroom.intel.com/news-releases/intel-drone-light-show-breaks-guinness-world-records-title-olympic-winter-games-pyeongchang-2018/#gs.ujzf9>.

3.5 INTERNET-OF-THINGS AND 5G NETWORK TECHNOLOGY

A 5G network is the catalyst for new capabilities like the Internet-of-Things, AI and quantum computing, and therefore offers hybrid actors an attractive target for sabotage and hacking.

The upcoming 5G network technology will potentially enable a diversity of hybrid threats. Technologies like AI and quantum technology require speed, latency and bandwidth, which will be offered by 5G. This offers a huge potential for e.g. boosting synthetic realities that go beyond current deepfakes. The foreseen fully connected and sensorized world as created by the Internet-of-Things can only be realized when 5G networks are commonplace. Likewise, the expected potential of quantum computing, which would enable the cracking of crypto, can only be exploited by 5G or even the after-next generation of networks.

The downside of this evolution is that our societies will become more vulnerable. In our interconnected societies and world, cascading effects will become more likely. However, the risks posed by IoT advancements does not only pertain to the interconnectedness between systems, but also the way in which they are integrated into everyday life.

Hackers target individuals through Amazon Ring devices. In December 2019, multiple users of Amazon Ring home security cameras reported hackers had gained remote access to their Ring devices and were eerily harassing them through the speakers installed with the camera. An eight-year-old girl was targeted in her bedroom whilst the hackers spoke to her about her surroundings and yelled racial slurs. Whilst this incident and similar events pertain to cybercrime, hacking and harassment currently, it is not difficult to imagine states using such technology to conduct psychological warfare in future. In 2014, Russians allegedly sent harassing text messages to Ukrainian fighters in the Donbass saying they would hurt their family if they continued to fight. This same psychological tactic could be used to harass and demoralize opponents, except instead of receiving text messages, the messages could be received over loudspeaker in your own home, with the adversary watching victims interact with their surroundings and family.

Developing 5G technology comes with a cost. The technology is more complex than its predecessors and requires a denser coverage of base stations to provide the expected capacity. This requirement makes it extremely costly and therefore risky for leading companies, since the 'winner takes it all' principle would allow the first 5G provider to set the world industry standard, thereby creating a strong leading position with possible monopolistic characteristics. Currently, the Chinese company Huawei is the leading party, but companies like Ericsson and Nokia are still in competition. This poses a dilemma for the EU and its member states who must choose a service provider. Whilst Huawei can probably deliver 5G networks faster than the other companies, as a Chinese company, this option generates specific risks. China's National Intelligence Law from 2017 requires Chinese organizations and citizens to "support, assist and cooperate with the state intelligence work." Therefore, it is believed that Huawei could be forced to hand over 5G data to the Chinese government, if so required.



Countries deciding to go along with Huawei would therefore risk being exposed to Chinese espionage. It would even give China the option to shut down specific IoT applications and networks, for instance as a coercive tactic in a conflict or dispute. Even though this is not yet reality, this discussion foreshadows possible future scenarios.

3.6 SATELLITE JAMMING, SPOOFING AND HACKING

Societies will increasingly depend on satellite services, making satellites an interesting target. Technologies for jamming, spoofing and hacking of satellites will become more commonplace.

Our societies have become highly dependent on satellite navigation and communication. A disruption to these satellites can have serious consequences for basic utility functions, such as communication, transport and financial transactions, leading to societal chaos within days. Many critical sectors depend on satellite navigation and do not have a back-up for global positioning. Navigation satellites also pass a time signal through with an accuracy to the billionth of a second. This time stamp is used for numerous processes within various sectors, for example in the financial sector. In banking, it is crucial to have an exact and reliable time stamp for successful money transfers and stock exchanges. New developments like the introduction of autonomous cars and trains are only feasible due to precise timing and positioning. Our dependence on satellites make them a viable target for actors to compromise.

GPS disruption at Israeli airport

On June 25, 2019 the Israeli airport Ben Gurion in Tel Aviv experienced GPS disruptions in its airspace. Over a period of three weeks, many pilots had lost satellite signals from the Global Positioning System around the airport. According to the Israeli Air Force, the unknown disruption of the GPS signal came from Russian actors in Syria. While the Russian ambassador to Israel called it “fake news” which he “cannot take seriously”, Todd Humphreys, professor of satellite navigation at the University of Texas, confirmed the Israeli’s accusation. Humphreys stated on the news site c4isrnet.com that Russia can broadcast a unique combination of signals that disrupt the real GPS signal (jamming) and at the same time generate a false GPS signal (spoofing).

Satellites are naturally vulnerable as they can be accidentally hit by space debris, or their signals be disturbed. However, there is also growing concern that satellites can be affected by intentional actions, like jamming, spoofing, hacking, espionage or even the use of physical weapons (which would certainly cross the boundary of armed conflict). Jamming is the intentional transmission of radio frequencies or signals to drown out the reception of satellite signals from space. Jamming equipment and knowledge is becoming increasingly available; hence the abuse of it, e.g. against satellites, is becoming more likely. Spoofing is achieved when a real satellite signal is replaced by a manipulated, more powerful signal that gradually deviates from the actual position or time, leaving the recipient with an incorrect signal. Although spoofing equipment is larger and more complex than jamming equipment and requires more knowledge and skills to operate, it is relatively easily available. Another weak spot for satellites is represented by cyberattacks, such as the hacking of satellites, which has been tried in 2017 by Chinese hackers that tried to gain control of U.S. satellites. With the growing number of satellites each year, partly an effect of the development of cheaper and smaller satellites, the risk of spoofing, jamming and hacking those satellites will increase.

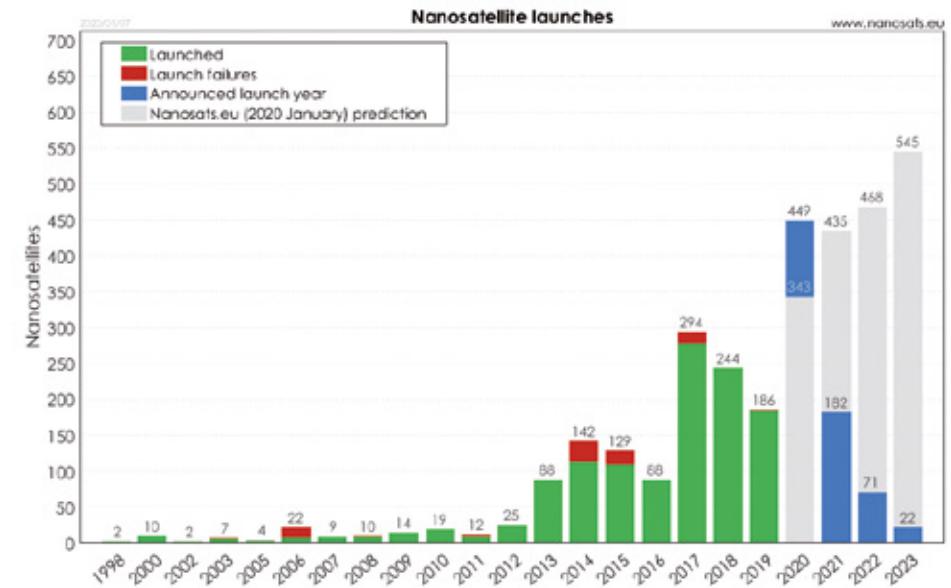


Figure 6: the number of nanosatellites launched over time.

The US National Security Agency (NSA) is currently studying satellite hacking while the U.S. Airforce plans to let hackers attempt to hijack an orbiting satellite during the 2020 Defcon hacking conference. The NSA is using AI to characterize strange behaviors in small satellites to understand if they’ve secretly been brought under adversarial control. The agency stated that several small satellites deployed to a very specific region in low Earth orbit are exhibiting unusual, anonymous behavior, suggesting serious compromise. Since humans are unable to consistently detect these compromises, AI could be helpful in that sense.

3.7 OFFENSIVE CYBER TOOLS

The evolution of cyber warfare and its tools is pacing on, new phenomena like co-option of hacking tools and bypassing two-factor authentication have just been born and will quickly become more widespread.

Cyber warfare can present a multitude of threats toward a state. At the most basic level, cyberattacks can be used to support traditional warfare, for example by tampering with air defense operations via cyber means in order to facilitate an air attack. Other physical effects that can be caused by the use of cyber means are the sabotage of critical infrastructure, (as occurred with the Stuxnet virus targeted against Iranian nuclear facilities) and economic disruption. The most devastating of the latter kind has been the WannaCry and NotPetya

cyberattacks in 2017. Masquerading as ransomware, these attacks caused large-scale disruptions in Ukraine as well as to the U.K.'s National Health Service, pharmaceutical giant Merck, shipping company Maersk, and other organizations around the world. Another example is the Shadowbroker's hack into the NSA, with the NSA toolset now being distributed and sold on the Internet.

Aside from these 'hard' threats, cyber warfare can also contribute towards 'soft' threats such as espionage and propaganda. A report from the Center for Strategic and International Studies (CSIS) and McAfee states that total cybercrime damage to the global economy is around 600 billion U.S. dollars annually (0.8% of global GDP), with cyber espionage accounting for 25% of this figure.²⁶ An example of cyber propaganda is the use of so-called 'information troops' by Russia to control information with the aim of undermining the notion of objective truth and reporting.

The evolution of cyber warfare and its tools is progressing, as has been seen by the co-option of hacking tools used by third parties and the use of AI to design undetectable malware and/or monitoring, detection and reconfiguration tooling. Not only does this phenomenon create sophisticated new tools by learning, adapting and re-emerging from other tools that had already been used in the past, it also makes attribution a challenge.

Co-option of hacking tools

On 22 October 2019, a joint advisory group from the U.S. National Security Agency and UK National Cyber Security Centre warned that cyber-group Turla (widely believed to be Russian) co-opted two Iranian hacking tools known as "Nautilus" and "Neuron" in order to target military, government, academic, and scientific organizations in at least 35 different countries. The advisory group indicated that the tools had "very likely" been acquired by 2018 through a range of mechanisms, including scouring the networks of victims of the two tools for backdoors inserted by Iranian hackers. According to the advisory group, "The timeline of incidents, and the behavior of Turla in actively scanning for Iranian backdoors, indicates that while Neuron and Nautilus tools were Iranian in origin, Turla were using these tools and accesses independently to further their own intelligence requirements. Iranian hackers were almost certainly not aware of, or complicit with, Turla's use of implants."²⁷

Bypassing two-factor authentication (2FA) has been a new tactic in cyber hacking, as was detected by the Dutch cyber-security firm Fox-IT in December 2019. Its security researchers say they found evidence that the attacks that bypassed 2FA have been attributed to a group which the cyber-security industry was tracking as APT20, believed to operate on the behest of the Beijing government. The group's primary targets were government entities and managed service providers active in fields like aviation, healthcare, finance, insurance, energy, and even in niche areas such as gambling and physical locks.

Another gamechanger in the cyber domain could be quantum computing. Quantum computers are based on a very different approach to storing and processing information than present

computers, enabling exponential processing power. With algorithms on a quantum computer cracking the security of a 3,072-bit RSA key can be reduced to only about 26 bits. One can easily crack a key that provides only 26 bits of security with the computing power of even a cellphone. If engineers figure out how to build large-scale quantum computers, the security provided by the RSA algorithm essentially disappears, as does the security provided by many other common public-key encryption algorithms, including those based on elliptic curves.

China is catching up with the U.S. in the quantum computing race and is likely to exceed the capabilities of the U.S. in the near future. It is reportedly investing ten billion U.S. dollars in building the National Laboratory for Quantum Information Sciences in Hefei. China's quantum ambition has parallels with similar investments in artificial intelligence, and stems partly from a desire to position the country as the technological leader of the decades to come. Interestingly, China is putting emphasis on quantum communications, in which it already seems to be ahead of the rest of the world. With Quantum communications, it would be possible to secure information and making it virtually impossible to be hacked. Consequently, it comes down to who will be the first to secure its information by quantum communications whilst having the capability to crack all other's information using quantum computers.

3.8 MICRO AND PRECISION TARGETING

Technologies to target individuals and small groups with the aim to influence or physically harm will become more advanced. Neurohacking and lethal micro drones are emerging.

Precision marketing techniques are already present example of micro and precision targeting. These techniques will empower not only marketing strategies for companies but also hybrid operations by state actors and proxies. Specific people or groups of people can be targeted in order to influence their opinion about political sensitive issues or to stir up societal polarization between groups.

It is expected that within a decade those techniques will make it possible to consistently influence and target individuals with highly customized messages. Such techniques will be employed through social media platforms, but also increasingly through other means, targeting individuals whose online behavior generates trails of data through their mobile phones, internet browsers and their online shopping preferences. Advancements in 'neurohacking'²⁸ for example, will facilitate new capabilities in 'neuromarketing', which targets people by manipulating their desires and needs through marketing and advertising that appeals to their mental state and emotional inclinations in real time. Facial recognition analysis technology will be able to gauge the emotions of several million users in multiple countries; emotion metric algorithms will be able to aggregate and interpret those emotions from facial recognition software. Artificial agents linked to facial recognition systems and algorithms that can engage with people virtually will also become widely used marketing tools and data collection mechanisms by 2035.²⁹

²⁶ James Lewis, 'Economic Impact of Cybercrime - No Slowing Down' (Washington D.C., USA: Center for Strategic & International Studies, February 2018), <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?k=1HywrewRzH17N9wuE24soo1dhuHd>.

²⁷ Jack Corrigan, 'Russian Hackers Co-Opt Iranian Cyber Tools to Attack 35 Countries, NSA Warns', Nextgov.com, 22 October 2019, <https://www.nextgov.com/cybersecurity/2019/10/russian-hackers-co-opt-iranian-cyber-tools-attack-35-countries-nsa-warns/160756/>.

²⁸ Neurohacking is the colloquial term for neuro-engineering and can be seen as a form of biohacking focusing on the brain and central nervous system. Strictly speaking it is any method of manipulating or interfering with the structure and/or function of neurons for improvement or repair. [<https://en.wikipedia.org/wiki/Neurohacking>]

²⁹ Michael J. Mazarr, 'The Emerging Risk of Virtual Societal Warfare', Research Reports (California, United States of America: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html.

Next to influencing specific individuals, it will become possible to physically engage or disable specific individuals or components with surgical precision. By combining behavioral information about specific individuals obtained from social media with geospatial information provided by an increasing sensory environment, it will become more and more mainstream to precisely locate individual people at any time. Physical targeting will then become the next step, for instance by employing micro- or nano-drones equipped with effectors such as deadly poison, anesthesia and immobilizers.

The concept of precision targeting or micro targeting (the latter is commonly used in reference to marketing campaigns and influencing voters during election campaigns) can also be employed for surgical precision attacks against infrastructure or platforms, for instance to cut the power supply cable of a radar system with a remote-controlled robot. This allows hybrid actors to stay below the threshold of war, not using bombs or missiles but robot systems which will be hard to detect and attribute to the attacker.

Other means that can be used to damage or neutralize infrastructure and platforms with high precision are smart jamming against systems that use the electromagnetic spectrum (radars, communication systems, drones being remotely controlled) and cyber weapons.

Russia employing small drones for targeting ISIS individuals

In July 2019, the Russian Ministry of Defense told news site Izvestia that it would supply troops with small drones that will eventually be able to drop bombs. It constitutes Russia's response to ISIS attacking Russian forces with small bomb-rigged drones in Syria in 2018. Russian law enforcement agencies already use small drones, but what's new is Russia's decision to weaponize them. It is unclear how large the drones will be, or how many of them Russia will utilize, but according to CNA Corporation (the US Centre for Naval Analyses), it might be possible that the Russian drones can be used to target individuals or small groups and remain very difficult to detect and interdict.



4 SYNTHESIS

It is now easier than ever for states to break their adversary's resistance without fighting. States attempt to do this using military, political, economic, information and cyber tools that fall below the threshold of armed conflict.

In the military domain, foreign special ops operatives that e.g. plan and execute assassinations remain a threat in Europe. Criminal groups, paramilitary organizations, private enterprises and state-supported/owned entities continue to operate as proxy actors for states seeking to avoid direct contact with conflict. States continue to send powerful and provocative messages by conducting aerial and maritime intrusions and staging military exercises near borders. Interference with the political affairs of foreign states can be expected to occur in the coming years too, especially during election times. Notable elections in 2020 prone to interference include the Taiwan General election, the Hong Kong Legislative election, the French Senate elections, the Greek presidential elections and the United States Presidential elections.

Economic coercion is set to become even more widely used. This will challenge the status quo under which international trade is conducted and will create further uncertainties for trade between states. In the information domain, advancements in artificial intelligence, virtual reality, augmented reality and machine learning will provide new opportunities for information manipulation. Cyberattacks will challenge our societal dependence on cyberspace and broaden the range of systems considered as critical infrastructure. Due to increased demands for national sovereignty, some states will enforce national governance of the internet, making it easier to threaten or attack other's internet infrastructure.

New and emerging technologies create new capabilities, with the potential to intensify and revolutionize hybrid conflict.

Such technologies will certainly become manifest in the

information domain, but not only there. Additive manufacturing and autonomous systems will provide terrorists, criminal groups and paramilitary organizations with new options for physically targeting specific people and vital assets without the risk of attribution or being in the danger zone.

In general, three overall trends can be observed. The first is that new parties are emerging as prominent proxies in hybrid conflicts. Although many of the examples used here pertain to Russian, and (to a lesser extent) Chinese actions, smaller, and indeed Western, states as well as a variety of non-state actors (whether as proxies or not), are set to use hybrid instruments that are difficult to counter. The second overarching trend pertains to the widening geographical scope of hybrid conflict. Russia, China, Iran and North Korea will remain posing hybrid challenges to the West. However, hybrid threats and conflicts will manifest worldwide, which current examples in Latin America as a case in point. The final general trend is the way in which new technologies, foremost artificial intelligence, could potentially intensify and revolutionize hybrid conflict.

Overall, hybrid tactics will remain a dominant shaper of competition and conflict for at least the next five to ten years, and will continue to add complexity to world affairs.



TNO innovation
for life

TNO.NL

20-11350 february 2020

