Hybrid Conflict: The Roles of Russia, North Korea and China

Edited by: Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt

Clingendael Institute

A report by the Dutch National Network of Safety and Security Analysts (ANV)
May 2018

Hybrid Conflict: The Roles of Russia, North Korea and China

Edited by:
Frans-Paul van der Putten, Minke Meijnders,
Sico van der Meer and Tony van der Togt

A report by the Dutch National Network of Safety and Security Analysts (ANV)
May 2018

About the National Network of Safety and Security Analysts

This report is the outcome of a project conducted by the Clingendael Institute as a member of the Dutch National Network of Safety and Security Analysts (ANV) on behalf of the National Coordinator for Security and Counterterrorism (NCTV) of the Netherlands.

The ANV is a knowledge network that was established in 2010.

The ANV consists of a permanent core of six organisations surrounded by a network of organisations such as knowledge institutions, research agencies, civil services, safety regions, critical infrastructure sectors, private companies and consultancy firms which are engaged in the production of the National Risk Assessment (NRA) and underlying studies depending on the knowledge requirement. The permanent core consists of:

- The National Institute for Public Health and the Environment (RIVM)
- The Research and Documentation Centre (WODC), Ministry of Security and Justice
- The General Intelligence and Security Service of the Netherlands (AIVD)
- The Netherlands Organisation for Applied Scientific Research (TNO)
- The Netherlands Institute of International Relations 'Clingendael'
- The International Institute of Social Studies (ISS) of the Erasmus University Rotterdam

May 2018

Contents

Introduction

Frans-Paul van der Putten and Minke Meijnders (the Clingendael Institute, The Hague)

Hybrid conflict became a much discussed concept after the Russian annexation of Crimea in 2014. While the phenomenon itself is nothing new, the re-emergence of significant great-power frictions combined with new technologies such as those that enable the cyber domain, have triggered fresh evaluations of hybrid conflict and its impact on national security. This collection of essays is the outcome of a project conducted by Clingendael as a member of the Dutch National Network of Safety and Security Analysts (ANV) on behalf of the National Coordinator for Security and Counterterrorism (NCTV) of the Netherlands. The project's aim was to assess whether and how the concept of hybrid conflict plays a role in the foreign relations of Russia, North Korea and China, to explore what this implies for Dutch national security, and to increase awareness in the Netherlands of the latter. In March 2018, the essays in this report were presented and discussed in a series of three seminars that took place at Clingendael, with each seminar focusing on the mentioned countries, respectively.

There is no generally accepted definition for the term 'hybrid conflict'. This project follows the definition of hybrid conflict that is used by the NCTV: it is understood as conflict between states, largely below the legal threshold of an open armed conflict, with the integrated use of means and actors, aimed at achieving certain strategic goals. This type of conflict is characterised by:

1) The integrated deployment of multiple military and non-military means, such as diplomatic, economic and digital means, disinformation, influencing, military intimidation, etc., that belong to the toolbox of state instruments;
2) Orchestration as part of a strategy/campaign;
3) The intention of achieving certain strategic goals;
4) Important features, namely deception, ambiguity and deniability, which accompany the actions (or could do so), making it difficult to attribute them and respond to them effectively.

The rationale to focus on these three countries in particular was that Russia, North Korea and China are believed (by Western observers) to engage in various forms of hybrid conflict in parts of their home regions (Eastern Europe for Russia, South Korea for North Korea and East Asia for China). Moreover, these three countries have political systems that are based on values that contrast with those on which the Dutch political system is founded, and some of the presumed targets or counterparts of their efforts at hybrid conflict are either allies or allies-of-allies of the Netherlands. From a Dutch security perspective, this raises the question of whether these activities potentially affect the Netherlands. However, this selection of countries does not imply that the three selected countries should be regarded as similar in their foreign policy behaviour, or that they are the only three actors that potentially engage in hybrid conflict. Indeed, the United States and other major Western actors are also widely believed to have extensive track records in the domain of hybrid conflict.

Approaches to Hybrid Conflict

The three countries' approaches to hybrid conflict differ significantly in terms of their perception in Europe, aims and means. In Europe, it is the Russian case that has generated most attention, for instance because of the role of 'little green men' (soldiers in unmarked green uniforms) during the Russian annexation of Crimea in 2014, Russia's involvement in the military conflict in Eastern Ukraine, and its alleged meddling in American and European elections through the spreading of 'fake news' and via other means. While Russia's immediate neighbours are faced with a wider range of Russian

influencing tools, including military, in Western Europe (including the Netherlands) the most notable aspect of the way in which Russia engages in hybrid conflict relates to the shaping of public opinion. Over the past decade, the Russian approach appears to have shifted from being mainly defensive against Western political influence in Russia itself, to a more offensive stance. The picture that emerges from the contributions to this report is that major strategic aims underlying Russia's engagement in hybrid conflict include changing the balance of power in Europe (weakening the influence of the European Union (EU), the North Atlantic Treaty Organisation (NATO) and the United States (US) by destabilising democratic processes and institutions in European societies) and making the international system more favourable to Russia's political interests (by weakening the legitimacy and appeal of liberal values). As discussed in the contributions by Keir Giles, Stefan Meister and Tony van der Togt, notable means used by Russia include the spreading of disinformation, interference in political processes, cyber-attacks and leveraging economic influence for political means. While the direct impact of Russia's engagement in hybrid conflict on Europe remains hard to determine, it seems that Russia is increasingly sophisticated at exploiting vulnerabilities that result from the open nature of European societies and existing tensions among the member states of NATO and the EU.

Europe's perception of the threat of hybrid conflict with North Korea is limited, certainly when compared to Russia and China. North Korean efforts at hybrid conflict are targeted primarily towards South Korea, and to a lesser extent towards the United States and Japan. As Sico van der Meer, Namhoon Cho and Jenny Jun explain in their contributions, North Korea's government has long engaged in a wide-ranging and ever-changing mix of provocative tactics to exert political influence abroad, while avoiding a major military conflict. Significant aims include preparing for the eventuality of a continuation of the Korean War that ended with an armistice in 1953 and changing the balance of power on the Korean peninsula (by destabilising South Korea and its military alliance with the United States). Methods of hybrid conflict that have been used by North Korea include creating shock effects (for example, through terrorist attacks, localised military incidents, or missile or nuclear weapons tests) and involvement in transnational organised crime. One notable tool is the use of cyber capabilities. Over the past decade, North Korea has quickly improved its cyber capabilities and has become one of the world's leading cyber actors. Through the cyber domain, North Korea's engagement in hybrid conflict potentially has a global reach.

China's engagement in hybrid conflict is visible mainly in East Asia, for instance in the South China Sea where it makes use of ambiguity (for example, the extensive but only partially defined nature of Chinese maritime claims) and a gradual but persistent build-up of its law enforcement and military presence, which weakens the positions of other claimant states without triggering an armed conflict. Like Russia and North Korea, China engages in hybrid conflict to change the balance of power in its home region, for instance by attempting to weaken the regional influence of the United States. However, unlike the other two actors discussed in this report, the Chinese approach seems more gradual and aimed at the long term, and not at destabilising countries or the international environment. From a European perspective, Chinese activities related to hybrid conflict – such as those in the South China Sea – are often interpreted as unfavourable (undermining international law and increasing the risk of regional instability in Asia), but they are not seen as requiring urgent action. However, European perceptions of China's influence closer to and within Europe itself have recently changed. Partly because of China's rapidly growing global economic presence, European governments are increasingly paying attention to the possibility that the Chinese government (or rather, the Chinese Communist Party) exerts undesirable political influence in Europe. It is not clear whether or to what extent the term 'hybrid conflict' applies to relations between China and Europe, so the three contributions on China in this volume, by Matt Ferchen, Jan Weidenfeld and Frans-Paul van der Putten, discuss related aspects but avoid using the term itself. They address the question of whether and to what extent China uses economic, cultural and educational ties to exert political influence in ways that affect European national security interests. The main relevant aims for China in this regard seem to relate to China's domestic security (preventing foreign support for domestic political opposition), creating a favourable international environment (by undermining the international role of liberal values) and changing the balance of power between China and the United States (by bringing Europe closer

to China's position and widening transatlantic positions). Related tools include economic influence, political interference and cyber activities. However, it should be noted that it can be very difficult to distinguish between targeted and unintended or passive political influencing, and between accepted activities (such as public diplomacy) and those that harm national security. Still, targeted political influencing seems to have become an increasingly visible feature of China's engagement in Europe. It is primarily aimed at political and business elites, media and think tanks, but ultimately also at overall public opinion. Potential security risks are likely to be of a long-term rather than a short-term nature and relate to the weakening of European and the EU's global influence (through the erosion of economic competitiveness) and to the EU's ability to act as a unified actor and a close partner of the United States.

Hybrid Conflict and its Relevance for the Netherlands in Perspective

Notwithstanding the fact that the ways in which Russia, North Korea and China (among other countries) engage in hybrid conflict could affect Dutch national security, this should be seen in a broader perspective of conflicting and shared interests. While there are some important areas in which Dutch interests conflict with those of these actors (such as political values and security alliances), the Netherlands maintains diplomatic, economic and cultural relations with all three. China, in particular, is a country that is not perceived by the Netherlands as a military adversary, and that is a major and growing trade and investment partner. On the international stage, China is increasingly a potential for or actual partner of the Netherlands, for example with regard to fighting climate change.

Some observations emerge from this volume regarding the relevance for Dutch national security of the activities of Russia, North Korea and China in the sphere of hybrid conflict and political influencing. First, hybrid conflict and political influencing play a role in international relations that is neither new nor confined to situations that verge on a major conflict. It is a permanent feature of the foreign policies of Russia, North Korea and China (but also of the United States and many other countries). Second, the Netherlands is not the prime target for hybrid conflict operations by any of these three countries. In the case of North Korea, the Netherlands so far appears not to be a target at all. In the Chinese case, the Netherlands is among many secondary targets of political influencing, but it is questionable whether the term 'hybrid conflict' is applicable. Only in the case of Russia is the Netherlands a target, but still only one target among many, and it seems that Russia pays more attention to its immediate neighbours and to larger Western countries. Third, the relevance of geographic distance as a buffer against undesirable political influencing has much diminished because of the role of the internet and, in the Chinese case, the presence of Chinese economic and cultural actors within Europe and the Netherlands. The cyber domain, in particular, strongly increases the vulnerability of the Netherlands as an open, free and digitalised society.

During the seminar sessions at which this report's essays were presented, various experts stated that countries such as the Netherlands should respond to the negative impact of hybrid conflict and targeted political influencing by focusing on protecting weaknesses that are inherent in an open society and increasing resilience by enlarging awareness among policy-makers and the general public. Also the need for cooperation and coordination across various sectors of government was highlighted by various experts. Finally, perhaps even more so than with other types of national security threats, addressing threats from hybrid conflict and political influencing involves fundamental dilemmas that relate to the balance between openness and security.

The editors wish to express their gratitude to the authors, Kay de Jonge, Margriet Drent, Lauriane Héau, Carla Veltkamp, and Rebecca Solheim, for their contributions to this project.

The views expressed in the essays in this report reflect the opinion of its respective author(s); they do not necessarily reflect the views of the Clingendael Institute, the Dutch National Network of Safety and Security Analysts (ANV) or the National Coordinator for Security and Counterterrorism (NCTV).

Russia

1 Russia, Influence and 'Hybrid'

Keir Giles (Chatham House, London)

Definitions

'Hybrid' terminology, including the phrases 'hybrid warfare' and 'hybrid threats', remains prevalent in many NATO and national strategies, despite having acquired so many different definitions that the term is effectively useless. When considering Russia, an additional layer of confusion is added by the fact that since 2016, the phrase *gibridnaya voyna* – the literal translation of 'hybrid warfare' from Western discussion – has begun to appear in Russian writing as well. At present, anybody researching hybrid warfare and Russia may thus confirm the false notion that this is also a recognised concept in Russia itself.

The solution adopted by the National Coordinator for Counter-terrorism and Security – referring to 'threats to national security arising from hybrid conflict', where hybrid conflict is clearly defined – is entirely appropriate. Yet at the same time, it is likely that it will have to be constantly both explained and defended against less-precise formulations that have become embedded elsewhere.

Influence Operations within 'Hybrid'

Within this definition, undeclared conflict between states, as practised by Russia, utilises different combinations of levers of national power against different adversary states. This presents a challenge for NATO and especially the EU when considering responses, since member states' threat perceptions vary so widely based on their separate experiences.

Russia's immediate neighbours feel a wide range of economic, diplomatic, espionage, cyber and other measures, up to and including tools of convenience to cause disruption and expense for the target state, such as migrant dumping. In the case of Ukraine, Russia feels able to bring the whole range of available tools to bear, up to and including targeted terrorist attacks and murders, sponsoring an active insurgency and supporting it with regular cross-border armed incursions.

For states in Western Europe, a more limited range of tools is used. The United Kingdom stands out as an exception, because of the large number of assassinations carried out on its territory on behalf of the Russian state.[1] Other states in the neighbourhood experience Russian interference, primarily in the realm of information and influence operations. Here, Russia uses its own and third-party media outlets, cyber hackers, business interests, non-governmental organisations (NGOs) and government-organised NGOs (GONGOs), Russian-speaking communities abroad and sponsorship of political parties to undermine democratic processes and decision-making in individual countries, the EU and NATO.

'Fake news', the current fashionable term for disinformation, is just one aspect of this approach. The underlying approaches and principles of such activities are broadly recognisable as reinvigorated subversion campaigns from the Cold War era and earlier. The key difference in implementation is technological enablers, which enhance the reach, speed and precision of information operations and vastly reduce their cost.

1 Editor's note: This contribution was written before the attempted murder of Sergei and Yulia Skripal in Salisbury, England, which confirmed this trend.

The objective can be strategic, including effective regime change – as demonstrated in Russia's attempts to influence the outcomes of the US and French presidential elections. But at a lower level of ambition comes broad-based, long-term weakening and undermining of adversary societies overall, without necessarily any specific short-term goal other than increasing Russia's relative strength in a classic zero-sum approach.

Russian interference is thus often destructive, not constructive; it may not favour a specific outcome of a democratic process, but instead seeks only to discredit the process as a whole. Russia does sometimes seek to damage the credibility of specific political figures. But more generally, a key aim is to shake confidence in the stability and integrity of the adversary country and its institutions, and to sow confusion, doubt and distrust.

Russian Influence and Enhanced Forward Presence

Countries distant from Russia experience more direct hostile action when they establish a presence in the frontline states, for instance by participating in NATO's Enhanced Forward Presence (eFP) deployments.

Russia works hard to undermine eFP because of the programme's effectiveness at ensuring NATO solidarity with the Baltic states and Poland. The methods used show how Russia exploits seams and divisions in order to sow discord. Interaction between visiting forces and the host nation's civilian population, between different national contingents within the eFP battalions, between these contingents and public opinion in their home countries, and between the host nation and NATO all provide attack surfaces. As elsewhere, the message is tailored to the audience. For instance, Russia wishes to convince host-nation civilians not to trust the eFP forces, and to persuade those forces that the host nation is not worth defending.

Stories are planted portraying eFP contingents as an occupying force that makes the host nation less, not more safe. Simple narratives, such as visiting officers taking all the best available housing, form the background noise for higher-profile disinformation attempts, such as allegations of major crimes by NATO soldiers. In all cases, staged incidents and paid provocateurs can readily create confrontations with visiting troops, and there is likely to be a Russia-sponsored news crew on hand. When national contingents include substantial numbers of non-white troops, Russia can also play the race card: exploiting ethnic stereotypes among the homogeneous populations of the frontline states, while at the same time convincing visiting soldiers that these populations are inherently racist, hence undermining their interest in defending them.

Action against eFP is a subset of a much more significant objective for Russia: eroding NATO unity and, in particular, the commitment of the United States to European security. Achieving political consensus or leadership change that leads a target country not to support activation of Article 5 by NATO would be the ultimate prize for Russia. In addition, Moscow combats awareness and criticism of Russian actions across the whole of NATO in order to reduce threat perceptions, and to undermine institutional support for countermeasures and defence investment. Targeting both sides of the Atlantic, Russia aims to erode the effectiveness and cohesion of NATO as a whole, but also the legitimacy of the West as a normative force upholding a global order based on universal rules rather than force of arms.

Indicators and Warnings

Given the undeclared, deniable and holistic nature of hybrid conflict, any unexplained dysfunction in any domain could be an indicator of an incipient or ongoing attack below the threshold of open armed assault.

Specifically in the domain of information warfare, one strong indicator is stockpiling by the adversary of either capabilities or narratives. This can be detected without resorting to classified sources. Advances in trolling and internet bot sophistication, micro-targeting, compound attacks combining cyber with other forms of information attack and many similar developments have all been identified by independent researchers, long before they reached the public domain.

Preparations like these serve as strategic indicators of intent. Tactical signs of impending action include the activation of narratives or networks held in reserve, as well as unexplained service outages, or a spike in hostile activity that is attributed to or claimed by third parties. The remedy is cross-domain situational awareness, closely observing civilian as well as military targets for signs of interference.

Conclusion: Responses and Recommendations

The first and most effective response to hostile subversive destabilising activity is, and always has been, raising public awareness. Statements recognising the state of conflict by senior figures such as prime ministers or defence ministers have been shown in the frontline states to be a powerful tool in empowering not only government, but also society and media to take steps to protect themselves. As a subset of this, attacks must be publicised, especially those that seek to exploit social divides. It is important to let the targets and vectors of hostile information campaigns know that they have been duped.

In addition, the following specific countermeasures should be undertaken:

- Enforce existing laws and regulations that are intended to ensure that media reporting is objective and accurate, whether nationally or on a pan-EU level. Apply laws that are designed to counter the spread of hate speech to disinformation from Russia, whether on traditional or social media.
- Publicly challenge ‘agents of influence’: politicians, academics, businessmen or journalists who promote Russian interests and narratives. As far as possible, make public counter-intelligence findings on who is being funded, encouraged or induced to promote Russian narratives in the media or academic discourse.
- Ensure that hostile disinformation does not cross from public-opinion space into policy-making space by means of monitoring and verification. Just as antivirus software protects a computer by ensuring that contaminated data introduced from outside does not affect core processes, so information-security programs should ensure that the sources of policy input are not corrupted by foreign influence.
- Emulate resilience measures by the frontline states beyond the information domain. These include bolstering capacity for swift responses by well-prepared law enforcement agencies, with permissive rules of engagement, in order not to cede escalation dominance in the case of unrest or insurrection sponsored from abroad. In the longer term, address and engage with social issues before the adversary does.
- At all stages, ensure the resilience of communications. It is vital for any Western government to ensure that in times of crisis with Russia, it can talk to its own people despite interference measures seeking to prevent it from doing so.

Finally, deterrence plays a critical role. The Obama administration’s response to Russian strategic information operations demonstrates that a failure to deter, whether by punishment or by denial, is the greatest provocation for Russia to engage in increasingly overt and aggressive action. The boundaries of acceptable behaviour need to be determined and communicated, along with the likelihood of countermeasures. The surest way to prevent Russia from waging hybrid conflict is to show that the costs of doing so will be too high or the rewards too low.

2 Disinformation as Part of Russia's Security Strategy

Stefan Meister (DGAP, Berlin)

Background to Russia's Disinformation Campaign

Russia is a latecomer to develop an updated strategy on shaping the global information sphere, unlike its use of cyber-attacks, which have been instruments of its security policy since the 2000s (for example, Estonia in 2007). The Kremlin failed to dominate the national or international discourse on domestic issues such as the Beslan terror attack in 2004, or during the Russian–Georgian war in 2008. The catalyst for a more comprehensive information strategy was the mass demonstrations in Moscow and St Petersburg in 2011–2012, which the regime interpreted as being inspired from the outside, mainly by the United States. That was the moment when Russia started to invest heavily in a disinformation and cyber strategy based on the view that in the 21st century, traditional security policy has to be linked with the domination and manipulation of the information sphere.

Disinformation is therefore a security strategy and part of the hybrid warfare that Russia's general staff and intelligence services have developed since 2012–2013 after the return of Vladimir Putin to the presidency. Feeling under attack by the West, Russia's leadership reacts from a position of weakness, using cyber-attacks and disinformation to counter Western soft power and to compensate for conventional strategic weakness. The so-called colour revolutions in the post-Soviet countries, together with the mass demonstrations of 2011–2012 in Russia, are the main reasons for this perception of vulnerability and threat by Russia's leadership.

The Russian authorities therefore see their policy as a tit-for-tat response to Western activities. However, while in the beginning Russia had a much more reactive than an offensive strategy, since disinformation has been so successful in confusing Western governments and societies, a more proactive approach has developed. This includes a shift by Russian international media outlets such as RT and Sputnik from presenting Russia to the world to giving a different perspective on negative developments in Europe and the United States. Manipulation of public opinion in the West via social networks, troll factories and bot nets, while boosting anti-US, anti-NATO and anti-elite narratives, is part of this policy.

Russia's disinformation strategy functions by trial and error. It is tailor-made to every target country, focusing on the narratives and bad news that work best in any particular environment. Many of the instruments used to influence publics and to discredit politicians, experts, institutions and the media in the West have been tested before in Russia and the post-Soviet countries. At home and abroad, the system often operates in a public–private partnership with Russian businessmen, as well as through the co-opting of 'independent' hackers by the intelligence agencies. It first tested and developed at home all the practices and tools that have been later used abroad, especially since the Ukraine conflict.

The main aim of Russia's disinformation in the West is not, above all, to help elect Kremlin-friendly politicians (even if this seemed to be the case in France with presidential hopeful François Fillon in 2017); it is rather to reduce the credibility of governments and politicians, as well as to disrupt the functioning of democratic institutions or the media. For example, the Russian state and its security forces use cyber-attacks to obtain information about leaders who they consider to be opponents, making the information public via WikiLeaks. The Kremlin's policy is also very much about showing

the Russian audience that the West is no alternative to the Putin system – that is, that the West is dysfunctional and unreliable – and that it is good to have Putin as a president who guarantees stability. Moreover, it is also about building up globally an alternative paradigm to the Western liberal values' system.

Germany as a Target of Disinformation

The EU countries, and particularly Germany, are important targets of Russian disinformation and cyber-attacks. In the case of Germany, the reasons are the leading role of Germany's Chancellor Angela Merkel in the Ukraine conflict and on sanctions against Russia, as well as Germany's crucial importance for the EU's stability. Typical paradigms of disinformation in Germany are topics such as the Second World War and fascism (guilt complex), American aggression (targeting the pacifist part of society) and resentment of the United States, opposition to NATO, migration and radical Islamism.

Instruments of Russian disinformation in Germany include:
- Russian international media such as *RT*, as well as its national branches like *RT Deutsch*, the media platform Sputnik and internet trolls.
- Russian security services, which work with co-opted hacker groups such as Fancy Bear in cyber-attacks to gather sensitive information.
- Increasing connections with left- and right-wing populist parties and groups like the *Alternative für Deutschland* (AfD) and the anti-Islamic movement PEGIDA, but also with parts of *Die Linke* party.
- Putin- and Russia-friendly national and regional (business) networks in Germany, which have been built up in the last fifteen years and now argue in the mainstream media for lifting sanctions and recognising Russia's annexation of Crimea.

Russia's international media is not in itself its most successful instrument of disinformation in Germany; it is rather a niche product targeting particular groups. Much more important is the growing interconnection between Russia's international media and Germany's (right- and left-wing) populist groups, parties and the peace movement – and also the instrumentalisation of minorities, such as the Russian-Germans with the 'Lisa case' in 2016. The content of Russian disinformation is spread through these groups and social networks with increasing success. Meanwhile, the number of interviews with representatives of the AfD, PEGIDA or *Die Linke* on Sputnik or *RT Deutsch* is out of proportion to their importance in the national discourse.

At the same time, there is a Kremlin policy to connect increasingly Germany's right-wing populist and anti-liberal groups with Russian institutions and actors. This includes links between the youth organisation of the Kremlin party United Russia with the youth organisation of AfD, or the legitimisation of Russia's Ukraine policy by inviting members of the *Die Linke* party to the occupied territories in Donbas in February 2015. AfD is the only party that had a social media campaign in Russian during the last German federal election in 2017, targeting Russian speaking minorities and German Russians, which all together make up more than 3 Million people.

The main challenge is not that Russia's media and security services have highly sophisticated new instruments to influence the German or European public; it is how they use and promote existing anti-US, anti-EU, anti-media, anti-establishment and anti-migrant feelings. Most elements of the narratives pushed by Russia already exist in growing parts of European societies, which criticise the inability of the governing elites to solve their countries' problems in an increasingly complex world. This self-doubt is supported by Russia's international media, whose main goal is to 'build up a counter-public as well as show media manipulation' in the German public discourse.[2]

2 See the self-description of *RT Deutsch* on its website: https://deutsch.rt.com/uber-uns/.

The 2017 German Election Campaign

Parts of this toolbox were used in the campaign for the Bundestag elections in 2017, although the Russian effort during France's presidential election earlier in the year – with fake news and attacks on Emmanuel Macron – seems to have been much more comprehensive. One of the biggest fears in German political and security circles was use of the contents of a 2015 cyber-attack on the Bundestag to influence the electoral outcome. As a result, while there was no big Russian disinformation effort during the campaign, there was an indirect impact on the public debate through the threat that it could happen. Russia's elites understood that Germany is much more stable than France, that its political discourse is less polarised, and that support for Chancellor Merkel was strong enough to resist any comprehensive attack.

Germany's decision-makers for a long time underestimated Russian disinformation. The cyber-attack on the Bundestag and the Lisa case were wake-up calls. Since then, different institutions have focused on the issue, including the Federal Intelligence Service, the Federal Office for the Protection of the Constitution, the Foreign Office and the Ministry of the Interior. According to news reports in January 2018, there is a plan to establish a centre for defence against disinformation at the Ministry of the Interior.[3] But the main challenge is that the attacks are comprehensive – linking foreign, domestic and security policy – and therefore every ministry has its related tasks and focuses, thus making it difficult to coordinate responsibility. For instance, in the ministry of foreign affairs, a new department for strategic communication is also dealing with particularly (Russian) disinformation. As a direct reaction to hate posts, fake news and social bots, the German Ministry of Justice approved a controversial law on 1 January 2018, which obligates the big social networks to delete or block 'obvious illegal content' within 24 hours of a complaint.[4]

What to Do?

- Improve the quality of media and investigative journalism, as well as the transparency of sources of information.
- Invest in analysis of disinformation, fake news and cyber-attacks worldwide, and explain to societies how disinformation works through media, think tanks and politicians.
- Strengthen resilience: Western societies and governments need to do their homework in terms of reforms, social demands and the roots of growing populism.
- Find the right balance: Not to build up Russia's disinformation campaign into something stronger than it is, as in the United States after the election of Donald Trump, and not to panic about Russia's disinformation, but to take it seriously.
- Improve the coordination of countermeasures with institutions and civil society nationally, among EU member states and institutions, and with NATO on cyber.

3 'Bundestpresseamt will Fake News strafrechtlich nicht bewerten', 15 January 2017, http://www.faz.net/aktuell/politik/inland/kein-zentrum-gegen-desinformationen-im-bundespresseamt-14652042.html.

4 Netzwerkdurchsetzungsgesetz, https://www.buzer.de/s1.htm?g=NetzDG&f=1.

3 Hybrid Conflict in Dutch–Russian Relations

Tony van der Togt (the Clingendael Institute, The Hague)

In discussing Russia's involvement as a state actor in hybrid conflict with neighbouring countries and the West in general, two distinct forms can be identified:

- Hybrid war proper: the 'use of political means to prepare the battlefield before direct military action' in the context of the so-called '*Gerasimov* doctrine';
- Political warfare: 'the pure use of political methods to bring about desired changes in policy in another state'.[5]

This essay focuses on the second form of hybrid conflict: Russia's attempts to influence policies in other countries, using a wide scope of possible channels in politics and societies.

Russian Strategic Aims in Influencing Western Policy

In general, Russia's attempts to influence other countries' policies are nothing new. However, what is new is the use of the internet and social media, providing for instant and targeted messaging, including the deliberate use of disinformation. Also relatively new is the now dominant narrative in Moscow, according to which Russia is mainly defending itself against a hegemonic and more powerful West, which is allegedly denying Russia its rightful place in the world and is working towards regime change in Moscow by supporting the promotion of democracy, civil society and human rights. In response, Russia has developed its own distinct forms of 'soft power' and uses different kinds of proxies (including 'cyber mercenaries'[6]) in a kind of public–private partnership, which makes attributing actions to Russian state actors difficult and helps Moscow to escape accountability by plausibly denying such efforts. In recent years, Russia has increasingly gone on the offensive to actively promote influence operations abroad, in an effort to divide the West and undermine trust in the liberal–democratic order and institutions, as shown most clearly in attempts to undermine the US elections in 2016.

Channels of Russian Influence in The Netherlands

Although discussions in the Netherlands often focus on Russian disinformation and fake news, the scope for Russian influence operations is much broader and includes working through business channels, political parties and specific Russian-sponsored organisations. Investigations into possible Russian involvement in the shooting down of aircraft MH 17 over Eastern Ukraine, the Ukraine referendum and Dutch support for economic sanctions and for NATO's Enhanced Forward Presence seem to have been the main targets of Russia's influence operations in the Netherlands.

5 Mark Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's Non-linear Military Challenge Right*, Mayak Intelligence Report, 2016 (withdrawn, but due to be published in early 2019 by Routledge). See also Galeotti's papers on the ECFR website on Russia's political warfare and use of organised crime.

6 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge: Cambridge University Press, 2018.

Media: Disinformation and Fake News

Russia has been complaining regularly about an anti-Russian bias in Dutch mainstream media. Therefore, in the most important recent cases of Russian disinformation and fake news in the Netherlands, social media, *RT*, Sputnik and the use of alternative journalists have all been employed to discredit the independence and integrity of the investigations pertaining to the tragedy of flight MH17, shot down over Eastern Ukraine, as well as to undermine trust in the viability of an independent Ukraine, worthy of European support. However, the net effect of such efforts (including sometimes intensive 'trolling') seems to have been limited in the short term, but could have more long-lasting consequences when combined with growing popular support for populist movements/parties and increasing distrust towards authorities, the establishment and mainstream media, as embodied in a post-truth world, in which 'nothing is true and everything is possible'. So far, MH17 investigations and the Ukraine referendum are the clearest examples of Russian disinformation efforts in the Netherlands, as also noted in a recent staff report for the US Senate.[7]

Business and Legal Cooperation

As geopolitical instruments of its hybrid conflict, Russia also uses its state-owned companies, especially in the energy sector, in order to lobby against economic sanctions. The Netherlands is especially vulnerable in this sector, as Dutch aspirations to become a 'gas roundabout' could lead to increased dependence on Russian gas imports, and also explains Dutch business support for the Nordstream offshore natural gas pipelines. Bilateral business councils are used to promote a return to 'business as usual' and Dutch/Russian companies (together with the Russian Public Diplomacy Corps) are sponsoring the annual RusPrix Award to promote closer relations. In the Netherlands, no Russian-sponsored economic studies have so far been identified, thus supporting the Russian narrative that sanctions are mainly harming European economies. Another element, linked to business relations with Russian state-owned or state-supported companies, could be attempts to influence (arbitration) court decisions, as shown in a recent Yukos oil company-related case in Amsterdam. The possible political use of legal courts or law enforcement in Russia is often underestimated. Finally, the global role of Russian offshore funds, partially using Amsterdam for tax reasons, and links between the Russian state and organised crime, as indicated most recently in Spain, call for closer investigations in the Netherlands as well. The same applies to the possible use of internet hubs in the Netherlands and Dutch servers by Russian cybercriminals and 'cyber mercenaries', working for Russian state entities.

Political Parties Supporting the Russian Narrative

Russia's support for anti-establishment, populist, mostly far right (but also sometimes far left) political parties in Europe has become an established fact, proven by regular contacts with Russian parties and sometimes by financial contributions as well. In its hybrid conflict with the West, Russia uses such parties and movements pragmatically, whenever it suits its political agenda and without any ideological consistency. Parties could share Russia's agenda of promoting conservative values or show understanding for Russia's revisionism and more assertive foreign policies. Often they share a nationalist, anti-EU agenda and oppose anti-Russian sanctions or NATO's Enhanced Forward Presence. In the Netherlands, Russia has mainly focused on cultivating ties with the *PVV*, as its leader Wilders is looking at Russia as a potential ally against islamist terrorism and mass migration. This has been further elaborated in recent studies on the contacts and (potential) cooperation between Russian state

7 See the recent minority staff report for the US Senate: *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security*, 115th Congress, 2nd session, Washington, January 2018.

authorities, parties and other actors (like Eurasianist philosopher Dugin) and the European Far-Right.[8] So far, Russian parties do not seem to have identified *Forum voor Democratie* as a potential partner, although its leader Thierry Baudet shares at least part of the Russian narrative and recently invited a prominent pro-Russian Eurosceptic John Laughland to speak at a public event. However, during the Ukraine referendum campaign, Russian influencers were mainly working with the leftist Socialist Party, which clearly shows the pragmatic, basically non-ideological approach by the Russian side, when working with political parties and movements abroad.[9]

Russian-speaking Community in the Netherlands

Unlike in Germany, the Russian-speaking community in the Netherlands is rather limited (approximately 40,000), politically divided and spread across the country. The Russian Embassy regularly organises events for compatriots, sometimes also involving Russian schools or the Russian Orthodox Church. However, the intention to establish a full-fledged representation of *Rossotrudnichestvo* (the main Russian organisation working with compatriots) in the Netherlands and a Russian cultural centre in The Hague failed for financial reasons. Although individual Russian activists are sometimes involved in political debates in the Netherlands, including on MH17 and the Ukraine referendum, their influence on the broader discourse is limited.

Think Tanks, Universities and NGOs

In the Netherlands, Russia has not established its own think tank to influence political debates, unlike in Germany (Dialogue of Civilisations, Berlin) or France (Institute for Democracy and Cooperation, Paris). However, the Kremlin-funded Russkiy Mir Foundation for propagating Russian culture has managed to establish a centre at the University of Groningen, although this clearly refrains from promoting Russia's more political agenda. A Russian-funded Expertise Centre has been established, linked to a Russian students' organisation in the Netherlands, but both have limited capacity and no immediate political dividend in influence operations.

Conclusions and Recommendations

From a broader European perspective, Russian political influence operations in the Netherlands are neither very successful, nor as intensive as in Central and Eastern Europe or in bigger EU member states such as Germany and France. This lack of success can partly be explained by Russia's unwillingness to cooperate constructively on the MH17 investigations. However, this should not lead to any complacency, as a lot depends on political circumstances and potential opportunities. When confronted by Russian disinformation, the Dutch government should not refrain from holding Russian authorities publicly accountable, as there is clear proof of Moscow's involvement. It should also strive for a common EU (and NATO) response in countering Russian information warfare, irrespective of where incidents take place. The Netherlands would then expect the same solidarity from partners when dealing with Russian disinformation on MH17. On the other hand, the Netherlands should be more open to addressing economic relations with Russia from a broader European geopolitical perspective. This would also imply a more strategic look at energy relations, financial flows and links with organised crime, including cybercrime.

8 Stanislav Byshok, *Novaya Evropa Vladimira Putina*. Moscow, 2016; Anton Shekhovtsov, *Russia and the Western Far Right. Tango Noir*. London/New York, 2017 and the accompanying blog: www.tango-noir.com.

9 Minority staff report for the US Senate: *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security*, 115th Congress, 2nd session, Washington, January 2018.

North Korea

4 The North Korean Tradition of 'Hybrid' Provocations

Sico van der Meer (the Clingendael Institute, The Hague)

Introduction

Hybrid warfare strategies are currently a hot topic among military and security experts. The North Korean case shows that hybrid warfare is not, however, a completely new phenomenon. If one defines hybrid warfare as the integrated deployment by states of various means and actors in order to influence or coerce other states with the aim of achieving strategic objectives while avoiding actual armed conflict, North Korea has been using this strategy since the 1960s. In the past, this has also been labelled an 'asymmetric' or 'unconventional' strategy. Currently, however, the cyber dimension is a new addition to this strategy, which may contribute to the use of the new term 'hybrid'.

This essay describes the long-term aims and trends in North Korea's strategies and means for 'peacetime' coercion below the level of armed conflict to reach strategic goals, as well as the rationale behind them. It provides context for the subsequent two contributions by Namhoon Cho and Jenny Jun, which will be more in-depth and focus on two specific aspects of North Korea's hybrid strategies: the role of the armed forces; and the use of the cyber domain.

The Continuous Need for Tension

Since the Korean War (1950–1953, when approximately 1.2 million people were killed), during which North Korea tried in vain to unify both Koreas by military means, the North Korean regime embarked on a strategy of low-level, asymmetric, or hybrid warfare strategies. It had no other choice than to acknowledge that it would not in the near future be able to win any actual military conflict against South Korea and its ally the United States. The regime in Pyongyang thus decided to focus on a strategy of asymmetric means in order to achieve important aims *vis-à-vis* South Korea and the United States, while avoiding full-scale conflict.

The strategic aims of North Korea's hybrid warfare can be divided into two categories: foreign policy aims; and domestic aims. On the foreign policy level, the main goal of North Korea's hybrid warfare is deterrence. The regime in Pyongyang sincerely fears regime-change efforts from outside – not only from South Korea and the United States, but also from other regional actors such as China and Russia. To deter such efforts, North Korea continuously presents itself as a powerful military actor, an unpredictable and dangerous player. To reach this aim, so-called 'hybrid' methods are used alongside more usual deterrent policies such as massive investments in the armed forces, including the development of weapons of mass destruction. Provocations – military and non-military – are meant to signal that North Korea is so powerful that any attempt to threaten it will fail and end in bloody retaliation.[10] Alongside the aim of deterrence, these hybrid operations are meant to weaken North Korea's 'enemies', the idea being that any method that hurts the United States or 'US-occupied' South Korea implies increased strength for North Korea. Finally, hybrid warfare is deemed to create room

10 Terence Roehrig, 'Restraining the Hegemon: North Korea, the US and Asymmetrical Deterrence', in: Tae-Hwan Kwak and Seung-Ho Joo (Eds), *The United States and the Korean Peninsula in the 21st Century*, Aldershot: Ashgate, 2006, pp. 163–184.

for manoeuvre for the regime in foreign policy. It signals that international rules and norms of state behaviour cannot be enforced upon North Korea, that other countries will have to accept that the regime can act as it desires. One example is massive illicit trade by the regime to circumvent economic sanctions, which although in itself is a 'hybrid tool' to deal effectively with policies of foreign actors, it is also supported by the continuing provocations and threats so that these illegal activities are less likely to see any retaliation. Pyongyang also hoped, especially in the 1960s, that 'hybrid' activities might destabilise South Korea and in turn spark a communist revolution there, leading to unification. This hope was lost quite early, however, when South Korea's anti-communist sentiments proved to be very strong.[11] Since the 1970s, destabilisation has particularly been intended to hurt and weaken South Korea in order to increase North Korea's relative strength.

The domestic perspective is also important. North Korea's totalitarian regime uses the image of a dangerous enemy from abroad to maintain the support of its population. The enduring message to the population is: support this regime, because only these powerful leaders are able to prevent foreign invasion and oppression. Creating continuing tensions with the 'enemies' and showing the regime's military successes to counter them are necessary propaganda tools for this domestic aim – while at the same time these successes should not cause actual war, which the regime realises it would lose. Hence the North Korean regime's reliance on asymmetric or hybrid strategies, which provide the positive aspects of tension-creating activities, while forgoing the negative characteristics.

Evolving Types of Provocation

The actual North Korean means of hybrid warfare have evolved over the decades. Some means are no longer used, some are rather new, and some seem to be ever-continuing.

Terrorist attacks, in particular, were regularly used by North Korea in the past, while they have not been conducted since the 1990s. This is probably to do with the changed international perception of terrorism, which was more common globally in the 1970s and 1980s, but especially after the Lockerbie bombing in 1988, the tide turned and state-sponsored terrorism was much quicker to be condemned and retaliated against. North Korea immediately recognised this changing environment and ceased this kind of activity. A few examples of North Korea's terrorist attacks to hurt its enemies while remaining under the level of formal war are: the attack on the South Korean presidential residence in 1968; the attack on the South Korean President in 1974, in which his wife was killed; the bomb attack during a South Korean state visit to Burma in 1983, which killed, among many others, four South Korean ministers; and the bombing of a South Korean airliner in 1987, killing all 115 people aboard. The many kidnappings of South Korean and Japanese citizens in the 1970s and 1980s, often by using small submarines, are a separate issue, because the objectives of the kidnappings vary: some abductees had to train spies; others were kidnapped so that North Korean infiltrators could take over their identity; and in a few cases even movie directors and actors were kidnapped to give a boost to the North Korean film industry.[12] Murdering North Korean defectors and exiles abroad, for example Kim Jong Un's half-brother Kim Jong Nam who was killed with the extraordinary VX nerve gas in Malaysia in 2017, is also a distinct issue.

Military surprise attacks are being used regularly as well. Some of them are quite big, such as the shelling of a South Korean island in 2010 and the torpedoing of a South Korean naval vessel in the same year. Other surprise attacks are smaller but not less shocking to the 'enemy', such as the axe

11 Andrei Lankov, *The Real North Korea: Life and Politics in the Failed Stalinist Utopia*, Oxford: Oxford University Press, 2013, pp. 27–32.

12 Charles K. Armstrong, *Tyranny of the Weak: North Korea and the World, 1950–1992*, Ithaca, NY: Cornell University Press, 2013, pp. 235–239.

killing of two US soldiers in 1976 or the incidents in 2015 in which the North Korean military hid landmines along South Korean border patrol walking routes.

There is a thin line between provocative attacks and mere bullying. North Korea has made provocative bullying a tool as well. Examples include the opening of dams at border rivers, resulting in sudden floods that kill people on the South Korean side of the border, but also the regular jamming of Global Positioning System (GPS) signals, affecting air and naval traffic in South Korea. A rather new means of hybrid warfare, which to some extent more resembles bullying and vandalism, are cyber-attacks. Since the 2000s, North Korea has been accused of various cyber-attacks aimed at South Korean banks and media, etc., with seemingly no aim other than destabilising South Korean society for a brief moment. Cyber espionage and cyber theft of (security-related) information and money are regularly used as well – not only targeting South Korea and the United States, but also globally (for example, the digital bank robbery of US$ 81 million from the Central Bank of Bangladesh in 2017).

North Korea carefully conducts its 'hybrid' activities within certain limits, cleverly calculating traditional South Korean restraint from escalating any response to prevent actual war – which Seoul will win in the end, but not after suffering enormous numbers of casualties and damage. Moreover, North Korea knows well that South Korea will also actively lobby the United so as not to escalate any response towards a level of actual warfare. Holding the millions of inhabitants of Seoul – which is only 60 kilometres from the border – as hostages with its massive artillery has also proven a useful tool for North Korea and created room for manoeuvre since the 1950s.

North Korea also combines its hybrid operations with the tactic of denial. Even when there is hardly any doubt about the perpetrators, North Korea still denies any involvement. For example, even after an international investigation team concluded that a North Korean torpedo had hit a South Korean naval vessel in 2010, North Korea persisted that it was innocent. This seems to be an integral part of any hybrid strategy: dividing other actors by causing doubt about responsibility for the perpetrated activity and thus limiting international responses to some extent.

Finally, North Korea's most famous provocative tool – its nuclear weapons programme – is being used in a 'hybrid' way as well. While using nuclear weapons as a deterrent is neither new nor 'hybrid', the lack of secrecy around its nuclear programme is surprising. Long before its nuclear weapons were usable at all, the regime was using them as a tool of provocation – among nuclear weapons experts, North Korea is sometimes referred to as a 'nuclear exhibitionist'. North Korea's persistent threatening statements to use nuclear weapons that were not, in fact, yet usable were meant to frighten – and thus deter – perceived enemies as well.

Conclusion

The North Korean case may offer various insights about hybrid warfare in general. First, this phenomenon is not as new as it may seem. North Korea has been using hybrid strategies for many decades already, although they used to be labelled as 'asymmetric' or 'unconventional' in the past. Looking at this long-term use shows how effective these strategies are: for decades, North Korea has effectively used hybrid strategies to provoke, hurt and bully its perceived enemies, while at the same time preventing escalation to the level of actual warfare. While most of North Korea's hybrid warfare has been focused on its direct 'enemies' – namely, the United States and South Korea – illicit trade and cyber operations are being used on a global level.

Second, an important feature of North Korea's hybrid strategy and the means used is that they have been continuously adapted to the ever-changing circumstances, and as such they have not become outdated and still maintain their strategic value. This also shows that countering such hybrid strategies requires continuous flexibility. The broad variety of means, in combination with the often unpredictable

character of hybrid surprise attacks, mean that it is hard to prepare for dealing effectively with an adversary using such strategies.

Finally, the North Korean case shows that hybrid strategies are not only useful for big powers. They can also be effectively used for smaller states facing bigger enemies to deter and provoke, while preventing any undesired escalation to actual armed conflict that cannot be won.

North Korean hybrid warfare is particularly aimed at South Korea and the United States. The direct threat for European states is currently not very high, except for the destabilising effects on the economically important region of North-East Asia and global destabilising effects caused by activities such as the trade in illicit weapons and criminal operations such as digital bank robberies. Nevertheless, one can conclude that North Korea can be recommended as a prime case study on how to make hybrid warfare strategies a long-term success and on how difficult it is to counter them effectively.

5 Hybrid Warfare on the Korean Peninsula

Namhoon Cho (Korea Institute for Defense Analyses, Seoul)

Introduction

North Korea has maintained a military strategy centred on guerrilla warfare, hybrid warfare and *Blitzkrieg* for a long time.[13] For the strategy's execution, North Korea has invested in building up asymmetric capabilities such as nuclear weapons and weapons of mass destruction (WMD), missiles, long-range artillery, underwater capabilities, special force units and cyber units. North Korea has employed this strategy because it is deemed more effective for accomplishing unification under communism with the current situation on the Korean peninsula, which includes the stationing and deployment plan of US forces.

Therefore, if an incident occurs on the Korean peninsula, North Korean forces are likely to resort to hybrid and guerrilla warfare and *Blitzkrieg* by launching massive surprise attacks on limited targets, mainly using their asymmetric capabilities.

This essay examines three things. First, what are the environments in which North Korea employs its hybrid warfare strategy? Second, what are North Korea's tactics for realising the above strategy in both peacetime and wartime? Third, what solutions are needed to deter and defend against North Korea's strategy?

The Korean Peninsula's Strategic Environment for Hybrid Warfare

There are many reasons why North Korea has employed hybrid warfare. The first reason is a geographical feature of the Republic of Korea (ROK, or South Korea), wherein the capital Seoul, where one-quarter of the population resides, is approximately 50 kilometres from the Military Demarcation Line (MDL). As a result, Seoul can be easily attacked by North Korea's conventional weapons system, including long-range artillery. North Korea possesses a lot of long-range artillery and deploys 1,000 of them in the MDL region. They are deadly threatening, because most of them aim at the Seoul area.

On the other hand, the Democratic People's Republic of Korea (DPRK, or North Korea) could try to besiege Seoul by formatting a second frontline behind Seoul. For this, it could have its special force units penetrate the MDL or Northern Limit Line (NLL)[14] through land, air or water. North Korea possesses approximately 200,000 light-infantry uniformed personnel who are trained to penetrate the MDL. It is difficult to prevent North Korea's light infantries from penetrating the MDL, because the mountainous areas around the MDL make it difficult for South Korea's military to keep watch and guard. Also, those wide mountain areas allow North Korean special force units to execute guerrilla warfare easily near the Seoul area.

13 ROK Ministry of National Defense, *2016 Defense White Paper*, p. 27.

14 NLL is a disputed maritime demarcation line in the Yellow (West) Sea between the DPRK to the north and the ROK to the south. This line of military control acts as the de facto maritime boundary between North and South Korea.

In addition, North Korea could use aircrafts and ships to transport special force units. The DPRK possesses many weapons systems, which enables easy mobilisation of its troops behind the Forward Edge of Battle Area (FEBA) Line. Approximately 330 transport aircraft, including ancient Soviet Antonov AN-2s, can simultaneously carry about 4,000 soldiers (twelve soldiers each). Each soldier may bring a nuclear pack to attack critical facilities in major cities. In addition, more than 100 Landing Craft Air Cushion (LCAC) military hovercrafts, including the Kongbang class, can simultaneously carry 4,500–7,500 maritime Special Forces, who could easily reach South Korea's five north-western islands, as well as the metropolitan areas of Seoul and Incheon. The disadvantageous geographical features of Seoul would make it difficult for South Korea to execute solid retaliation against North Korea if it attacks. South Korea would not be able to attain 'escalation dominance' because of Seoul's geographic location and mountainous landscape.

The second reason for North Korea's hybrid warfare is that South Korea's social and economic environments are vulnerable to terrorism. South Korea is an economically advanced country that has many critical systems and infrastructures, and its high urbanisation makes it easily exposed to terrorism. Its advanced information technology environment also makes the whole country easily exposed to terrorism and cyber-attacks. In addition, South Korea's nuclear power plants are extremely vulnerable to any terrorism by North Korea. North Korea could create nuclear chaos in the ROK even without using its nuclear weapons.

The third reason is divided public opinion in South Korea on security issues. South Korea has a long history of confrontation between the left and the right. In addition, arguments voicing the pros and cons on the issues of engagement or pressure against North Korea still prevail. Also, some South Koreans want the ROK to be more independent from the United States in security matters. Disputes over the issues of the South Korea–US alliance, wartime Operations Control (OPCON) transfer,[15] Terminal High Altitude Area Defence (THAAD) deployment and the South Korea–US–Japan trilateral security cooperation still prevail, giving the situation some room for North Korea to manipulate South Korean public opinion. Moreover, the mishandling of cyber operations by previous governments makes South Korea's cyber operations untrustworthy.

The fourth reason is the stationing and deployment of US forces. Approximately 28,500 uniformed US Forces to Korea (USFK) personnel are stationed in South Korea, and more troops will be deployed from Okinawa, Guam and the continental United States if a contingency situation occurs. North Korea, which knows this well, would try to claim victory before more US troops are deployed to the Korean peninsula. This situation would compel North Korea to use nuclear intimidation as well as conventional weapons systems. North Korea, which would not want US intervention, would try to end the war as quickly as possible. As a result, North Korea would use nuclear intimidation by threatening the United States with detonating a nuclear weapon if US troops deploy to South Korea.

In addition, North Korea may execute hybrid warfare by not wearing military uniforms, because the US troops have difficulty in distinguishing North Koreans from South Koreans.

North Korea's Hybrid Warfare Tactics

North Korea executes various hybrid warfare tactics to take advantage of the above environment. First, in peacetime, North Korea is employing the dual-track tactic of provocation and dialogue to gain the upper hand in inter-Korean relations and to acquire economic gains and force the South Korean

15 Currently, the authority for wartime OPCON in the Korea theatre of operations (KTO) belongs to Combined Forces Command (CFC), whose Commander is a US four-star general. South Korea is advocating for giving authority to the ROK.

government to change its North Korea policy.[16] For example, in 2010, North Korea committed two acts of provocation against South Korea: the sinking of the ROK ship *Cheonan* by a torpedo; and the indiscriminate shelling of Yeonpyeong Island. However, since the beginning of 2011, North Korea has proposed the resumption of dialogue with South Korea through its New Year's Joint Editorial, as well as through combined statements by its government, party and organisations. In addition, on 20 January 2011, a proposal for a high-level inter-Korean military meeting to ease tensions was made through an open letter from North Korea's People's Armed Forces Command.[17]

Another example is found in 2015. North Korea continued to provoke South Korea while engaging in a deceptive charm offensive, by professing the desire to improve inter-Korean relations in its 2015 New Year's Address and in the statement by the National Defense Commission. However, on 4 August 2015, North Korea again provoked South Korea by using a wooden-box landmine in the Demilitarised Zone (DMZ), and on 20 August 2015, it fired artillery rounds, thus ratcheting up tensions. However, with the 'August 25 Agreement', the two Koreas reached a deal to hold high-level meetings in order to de-escalate the tensions.[18]

Second, North Korea prefers provocations whose origins are difficult to identify. The sinking of the ship *Cheonan* and cyber-attacks are such examples. These sorts of provocations prevent South Korea from executing rapid response and retaliation, because the origins of the fire are not easily identifiable. Also, North Korea restricts itself to limited provocations, thus making full retaliation by South Korea difficult. Moreover, the fact that Seoul is vulnerable to a DPRK attack gives North Korea 'escalation dominance'.

Third, in peacetime, North Korea executes psychological and information warfare to disseminate propaganda aimed at misleading South Korean public opinion. Tactics of nuclear intimidation or spin control may be employed. In wartime, on the other hand, North Korea may disseminate a rumour that the United States will not dispatch reinforcement troops. This could be done after occupying the five north-western islands following a surprise landing attack, in order to propose a cease-fire dialogue before the United States deploys reinforcement forces to the Korean peninsula.

Fourth, North Korea could perform nuclear intimidation.[19] In peacetime, it could utilise nuclear weapons as a tool of diplomatic coercion. In wartime, on the other hand, it could intimidate the combined forces by claiming that it will use nuclear weapons if: 1) the United States deploys reinforcement forces to the Korean peninsula; 2) the combined forces penetrate the MDL; and 3) South Korea and the United States do not join a North Korea-proposed cease-fire dialogue.

Fifth, North Korea could execute irregular warfare by formatting a second frontline behind the major FEBA line in order to overcome its disadvantage in regular warfare. For this, as already mentioned, North Korea possesses almost 200,000 soldiers from special force units, enabling sudden penetration of the MDL or NLL, as well as weapons systems for deep penetration, such as Antonov AN-2 transporters and Kongbang class hovercrafts. Using these forces and weapons systems, North Korea could, during wartime, form a second frontline and create disorder and chaos in South Korea.

Sixth, North Korea could perform cyber warfare against the ROK to cause South Korea's social infrastructure to collapse and to aggravate confusion. South Korea's banking network systems have been attacked several times. North Korea has recently been trying to build up capabilities in this area and to steal cryptocurrency by cyber hacking.

16 ROK Ministry of National Defense, *2016 Defense White Paper*, p. 22.

17 ROK Ministry of National Defense, *2012 Defense White Paper*, p. 26.

18 ROK Ministry of National Defense, *2016 Defense White Paper*, pp. 23–24.

19 Park Yong Tak, 'The Possibility of North Korea's Hybrid Warfare and the Development of Phases', *Defense Policy Study*, no. 27-4, 2011, p. 98.

Seventh, North Korea could carry out terrorist attacks on South Korea's nuclear power plant facilities, which would result in similar effects to a nuclear attack – a terrifying prospect for South Koreans. As South Korea has 24 nuclear power plants, which are collectively located in the south-east region, an attack by North Korea against the nuclear power plants would result in catastrophe.

South Korean Policies to Deter North Korea's Hybrid Warfare

South Korea's interest in hybrid warfare is recent. However, because North Korea has employed guerrilla warfare and *Blitzkrieg* for a long time, South Korea has prepared solutions to defend itself against such warfare. The ROK would try to employ the following measures.

First, at the national level, capabilities for responding efficiently and rapidly to strategic hybrid threats should be built up. Government-wide structures and organisations that can respond to mixed threats of nuclear attacks, cyber-attacks, terrorism and criminal disorder should be established. A concept on a national control tower should be clarified. The control tower should be harmonised with the office of the prime minister, who is responsible for 'Integrated Defense'. On the military level, both capabilities and organisations to deal with so-called K3 operations[20] should also be built up as soon as possible.

Second, on the military side, a joint planning, programming, budgeting, execution and evaluation system (PPBEES) should be considered to integrate all the components and to develop all the missions. Collaboration is very important in responding to hybrid warfare situations. Each component should therefore make an effort to increase operational linkages. A measure implemented following the Yeonpyeong shelling, which gives a Marine Corps commander control over naval and ground forces in the five north-western islands, is an example of the increased cooperation of the forces.

Third, strategic communication should be expanded to the civilian sector as well as the military sector. Victory in modern warfare is not attained by military capabilities. Capabilities in diplomatic, information, military and economics (DIME) areas are required to win a modern war. This DIME concept is particularly important under hybrid warfare environments. Strategic communication should be undertaken at any time to accomplish flexible and integrated responses.

Fourth, South Korea has established a new military doctrine called 'Proactive Deterrence' since the Yeonpyeong shelling. This doctrine stipulates that: 1) South Korea should retaliate with greater force than the attack it receives; 2) South Korea should attack supporting troops and command facilities as well as the origins of fire; and 3) South Korea should pre-emptively strike North Korean missile launch bases if any signs of missile launch are noticed.

Finally, a mix of capabilities between high and low, lethal and non-lethal, and regular and irregular, etc., should be allocated appropriately.

20 K3 operations refer to operations by: KAMD (Korea Air and Missile Defence); Kill-Chain; and KMPR (Korea Massive Punishment and Retaliation).

6 Lessons from North Korea's Cyber Operations

Jenny Jun (Columbia University, New York)

Introduction

How does North Korea use cyber means to achieve its political and military goals? Although North Korea's long-time stated goal has been to reunify the Korean peninsula under its rule, winning a conventional war on the peninsula had become unrealistic by the 1980s as the military balance *vis-à-vis* South Korea had started to reverse. Moreover, with the end of the Cold War, Russian and Chinese patronage of North Korea diminished, while the US–South Korean alliance grew stronger. In this strategic environment, North Korea needed to devise new ways and means to ensure regime security, deter foreign aggression and compel adversaries.

North Korea's answer to such a situation was to rely increasingly on asymmetric strategies and irregular operations, which include both the adoption of new capabilities as well as use of otherwise conventional means in new ways that exploit asymmetric advantages. One obvious avenue that North Korea took was to establish a nuclear and ballistic missile programme. Others, less often discussed, include the Korean People's Army (KPA)'s Special Operations Forces (SOF) and North Korea's early interest in electronic warfare. As Sico van der Meer and Namhoon Cho highlight in their essays, North Korea has had a long tradition of incorporating components of what is now termed 'hybrid warfare' into its military strategy. Likewise, North Korea's acquisition of cyber capabilities is also a natural extension of such efforts.

This essay illustrates past North Korean cyber operations to assess how the state is most likely to use cyber capabilities in peacetime and during conflict to achieve its ends. Lessons from the North Korean case will then inform implications for policy-makers facing hybrid warfare threats.

Peacetime Cyber Operations: Disruption and Coercion

Below the threshold of war, North Korea has been engaging for almost a decade in malicious cyber operations during peacetime, ranging from attempted blackmail of a civilian nuclear reactor to hacking cryptocurrency exchanges. Setting aside its efforts to generate foreign cash through cybercrime, North Korea's politically motivated activities can be broadly characterised as either disruptive or coercive.

First, North Korea's disruptive cyber-attacks are rooted in an old tradition of launching limited provocations aimed at undermining and destabilising South Korean society or the US–South Korean alliance without risking general war. Since 2009, North Korea's cyber-attacks have evolved from rudimentary distributed denial-of-service (DDoS) attacks and website defacements to more sophisticated operations, such as the 2013 coordinated hard drive wiper malware campaigns on South Korean banks and news media organisations, which demonstrate significant investment of resources and organisational capacity. It is important to note that these cyber-attacks are planned and executed by North Korea's Reconnaissance General Bureau (RGB), which was formed around 2009 in an effort to consolidate a wide range of intelligence, commando and sabotage operations. Units that have since been incorporated into the RGB were responsible for assassination attempts

such as the 1968 Blue House raid and the 1983 Rangoon bombing, and more recently events such as the 2010 sinking of the ROK navy corvette *Cheonan* and the 2015 DMZ mine crisis. The fact that North Korea's disruptive cyber operations are spearheaded by an organisation that has a track record of a wide range of covert operations indicates that North Korea's cyber capabilities may be just another tool that serves the RGB's broad strategic interests.

Second, North Korea may in the future attempt to make greater use of cyber means for coercing its adversaries, especially for issuing compellent threats. When considering how North Korea might get the United States or South Korea to do what it otherwise would not want to do, its options have been limited thus far. North Korea's positioning of artillery against Seoul or its missile and nuclear programme have been useful for deterring invasion, but less useful for compelling them to initiate an action. With cyber means, however, North Korea is exploring new ways to compel the United States and South Korea to meet its demands. So far, these attempts have yielded mixed results, such as with the 2014 Sony Pictures' hack, or the 2014 attempt to blackmail a South Korean civilian nuclear reactor. Some scholars have argued that cyber means are actually a poor coercive tool, mainly by assuming that cyber operations rely on secrecy and surprise, and that this creates a trade-off between communicating a threat before attack and the credibility that the attack will succeed.

However, these assessments may need to be qualified in the future with the possible use of ransomware and/or doxing that bypasses this trade-off. For now, North Korea seems to have used ransomware mainly for the purposes of extorting money, but there is nothing technologically barring them from using the same tool to make political demands. Also, attackers can threaten to leak stolen information in conjunction with a ransomware attack to increase the costs of non-compliance, such as some variants of the Petya ransomware that threaten to release documents at predetermined intervals until the victim complies. While there will be limits on extrapolating the analysis from the individual to the government level, there is a real possibility that smaller NGOs, human rights activists, or companies that deal with sensitive issues related to North Korea may be subject to such coercive attempts, especially if their work is heavily reliant on information systems or proprietary information.

Cyber-enabled Warfare: Operation Orchard and Decision Cycles

North Korea may also actively incorporate cyber capabilities into its military strategy and doctrine to support a broader conventional military operation in at least two ways. First, it may try to disrupt or degrade enemy C4ISR in conjunction with electronic warfare,[21] in an effort to 'level the playing field' *vis-à-vis* the United States–South Korean alliance. While the KPA simply cannot match the US and South Korean forces conventionally, it must still try not to fall too far behind an enemy equipped with state-of-the-art precision weapons and C4ISR capabilities. Their next best option is thus to disrupt or degrade either the system/networks or the information passing through it to decrease the precision or effectiveness of these weapons, which rely heavily on the transmission of information in a timely and accurate manner. In fact, a leaked 2005 KPA publication – *Electronic Warfare Reference Guide* – states: 'If one disrupts the GPS systems of US's precision-strike weapons, one can degrade its precision and lead it to strike another area', and 'We can defend our troops and assets against electronically guided weapons if one knows how it works and develops appropriate defensive measures'. There is thus reason to believe that North Korea's strategic thinking on electronic warfare extends to cyber warfare.

Such efforts to disrupt and degrade enemy C4ISR have the added benefit of boosting the effectiveness of one's own otherwise inferior weapons systems. For example, during Operation Orchard, a 2007 Israeli operation to strike Syria's Al-Kibar graphite reactor, the Israelis used a combination of cyber and electronic warfare not only to disable Syrian air defence radars, but also to manipulate its screen,

21 C4ISR stands for command, control, communications, computers, intelligence, surveillance and reconnaissance.

such that the Israeli fighter jets, which were not stealth aircrafts, were able to enter Syrian airspace unimpeded. While not all air defence networks can be easily compromised, considering such an operation is certainly a more cost-effective alternative than investing in stealth capabilities. Along the same lines, if North Korea is able to compromise portions of South Korea's air defence or missile defence systems, it may be able to make greater use of its otherwise severely outdated air force, artillery and missiles.

In fact, North Korea has already demonstrated that it is capable of conducting a combined operation that incorporates electronic warfare (EW) elements. During the infamous shelling of Yeonpyeong Island in November 2010, North Korea jammed South Korea's AN/TPQ-37 radar before opening fire. This meant that the South Korean military had to rely on pre-existing coordinates when returning fire, resulting in 35 out of 50 rounds falling into the sea. This provided the North Koreans with enough time to fire a second round of attack. This occurred despite the South Korean military's 2005 assessment that North Korea's EW capabilities were not a threat because the military already has various countermeasures and encryptions. Thus degrading and disrupting enemy C4ISR using cyber means provides North Korea with asymmetric advantages by rendering enemy precision weapons less effective and boosting the effectiveness of its own conventional forces. If North Korea has successfully incorporated cyber warfare into its strategy and doctrine in a similar manner, it is possible that the next conventional provocation will be preceded with a cyber-attack.

Second, North Korea may try to use cyber operations as part of a broader attempt to extend its adversary's decision cycles in the context of *Blitzkrieg*-style manoeuvre warfare. Although unrealistic today, North Korea historically wanted to fight a *Blitzkrieg*-style war supported by extensive rear operations by SOF and irregular units. This kind of operation relies heavily on manoeuvre warfare, where mechanised forces quickly penetrate enemy defences, race to the rear, then isolate and destroy the defending forces while irregular and light infantry infiltrate and disrupt the enemy's rear flanks. The key here is that by having a faster decision cycle than the adversary, fast-moving mechanised forces can manoeuvre quicker than the defence is able to confront and destroy the threat.

In the past, North Korea's military strategy tried to slow down decision cycles through rear operations by special operations forces and light infantry units. However, given the geography of the Korean peninsula, such rear units would be severely undersupplied, and infiltration would be difficult given South Korea's maritime superiority. If North Korea uses a combination of cyber and electronic warfare, however, such disruption could be achieved much more effectively and quickly, as long as North Korea has conducted significant operational preparation of the environment in peacetime. If the KPA still engages in strategic planning for potential war on the Korean peninsula, it is possible that they have moved towards the latter direction.

Policy Implications

Until recently, North Korea had rarely been a security concern for the Netherlands and NATO. However, cyber operations now transcend many, although not all, of the geographical constraints of coercive diplomacy. North Korea, despite having very few conventional capabilities for power projection, has nonetheless been able to conduct operations such as the Sony Pictures hacking incident and the WannaCry ransomware attack in locations as far afield as the United States and United Kingdom. Sophisticated cyber operations also utilise third party infrastructures to enable offensive cyber-attacks on other targets. These are indications that policy-makers should remain wary of developments in North Korea's cyber strategy and capabilities.

Policy-makers should also keep in mind that while North Korea may arguably be less technically sophisticated in cyberspace than the United States, Russia or China, there are also fewer options ex ante to deter North Korea both in and out of cyberspace and ex post to punish the state in response

to an attack. North Korea is not very reliant on cyberspace for its military, political or commercial activities, meaning that there is very little to hold hostage to deter North Korea from initiating such attacks, unless the victim is willing to escalate to another domain. This means that North Korea may be particularly emboldened by the perception that its adversaries lack credible means to retaliate against its cyber-attacks. North Korea may thus even enjoy a greater asymmetric advantage than states such as Russia or China.

Beyond North Korea, this case study presents a number of general implications for preparing against hybrid threats. First, cyber-enabled warfare, in the context of a broader conventional war, has the potential to 'level the playing field' inexpensively by decreasing the effectiveness of precision weapons and war-fighting capabilities that are heavily reliant on C4ISR, while boosting the effectiveness of an otherwise inferior force. Second, related to this issue, there is a strategic question about whether deterrence or resilience would be the best way to mitigate the negative consequences of such threats. If hybrid threats have been developed specifically to get around existing deterrence structures, it probably means that additional measures to deter an adversary in this space may only have marginal effects. Finally, further efforts should be expended on discussing how international law or norms can deal with the rights and responsibilities of third parties that are being used as transit states for offensive cyber operations.

China

7 China, Economic Statecraft and Policy Banks

Matt Ferchen (Carnegie–Tsinghua Center for Global Policy, Beijing)

Introduction

A new conventional wisdom is emerging among many policy-makers, think-tank researchers and even the business community in Europe and the United States that China is increasingly moving towards authoritarianism in its politics and towards mercantilism in its economics. This move towards more illiberal economics and politics in China should, according to this new transatlantic consensus, serve as a wake-up call after decades of ill-conceived or at least overly idealistic engagement with China that mistakenly assumed that China would move inexorably towards ever-greater economic and political openness. Such arguments on both sides of the Atlantic share a further commonality: they generally agree that Chinese foreign policy towards Europe and the United States increasingly makes use of a wide and diverse toolkit across political, economic, social and educational domains. While my colleagues will focus on a number of these specific issue-areas, this essay explains the role, and policy implications for Europe, of China's 'policy banks' as key financial instruments of Chinese economic statecraft.

A key aim here is to understand whether and how Chinese official international finance, as channelled through its policy banks, is an important component of Chinese influence in Europe. Tied to this, the essay considers whether the concept of 'hybrid conflict' is useful in understanding the behaviour and influence of Chinese policy banks in Europe and more broadly. To anticipate the key outcomes of this analysis, the essay argues that while China's provision of official international finance through its two main policy banks – the China Development Bank (CDB) and the Export–Import Bank of China (Ex–Im Bank) – is a key part of China's increasingly proactive foreign policy and economic statecraft, it would be misleading to view this phenomenon through the lens of 'hybrid conflict' per se. Instead, it is important for Dutch and European policy-makers to understand the goals, the impacts, as well as the limitations and challenges of China's policy banks both in the European as well as broader international contexts. Moreover, while China's policy banks are important components of China's comprehensive and increasingly activist global engagement, they are so far of greater importance in Europe's periphery and in efforts to develop Eurasian infrastructure and energy linkages.

An Emerging Battle of Frameworks: Mercantilism versus Peaceful Development

A key part of the new conventional wisdom about China's drift towards illiberalism in both its domestic and international affairs is the sense that China's market-oriented reform era, which began in the late 1970s, has come to an end. In domestic policy, the emerging consensus among many observers in the United States and Europe is that Chinese efforts to liberalise the economy further have stalled and that the state is instead consolidating its efforts to control markets and firms through a renewed emphasis on industrial planning. The corollary in international affairs is that China is increasingly seen, and described, as 'mercantilist', in that it pursues a combination of domestic and international trade, investment and finance policies that serve not just China's economic but also its geopolitical and diplomatic interests. China's Belt and Road Initiative (BRI), as well as industrial/technology plans such as 'China 2025', are increasingly viewed as a symbol of China's definitive move towards mercantilism.

It is no coincidence that the term 'geo-economics', which is meant to underscore the linkage between economic and geostrategic goals and tools, is increasingly applied to Chinese-led overseas initiatives and behaviour.

China has long sought to portray its foreign policy, especially its economic dimensions, in starkly different terms from the zero-sum, mercantilist picture that is now ascendant in Europe and the United States. Perhaps the most obvious sign of this is in China's ubiquitous reference to 'win–win' economic and diplomatic relations. More importantly, China's core foreign policy framework – that of Peaceful Development – has a political-economy logic at its heart: China needs a peaceful international environment in which to pursue its own development, and in turn China's pursuit of economic development will be an engine of economic opportunity for all its commercial partners, and the ensuing 'mutually beneficial' development will further underscore peaceful outcomes. This, at least, has long been the rhetoric and logic of China's foreign policy and it is also crucial for understanding why China's newly activist or aggressive, foreign policy places economic development initiatives at its core. In the context of 'hybrid' approaches to foreign policy, it is important to note that China does not see 'development' in only the narrow terms of 'aid', but instead as an inclusive mix of trade, investment, finance and infrastructure-building where the state has a strong role to play in supporting, promoting and controlling markets and business.

China's Policy Banks and their Importance for Europe

China's policy banks fall into the controversial space between claims of Chinese mercantilism and Chinese development-oriented foreign policy rhetoric and aims. Even in a country where banks are the key institutions in the financial system, and where the majority of banks are state-owned, China's policy banks play a special role. In terms of foreign policy, it is China's Ex–Im Bank and the CDB that have come to play the biggest roles. Both of these banks have been tools in China's 'Going Out' policies, which since the early 2000s have been aimed at increasing China's role in global trade as well as in overseas investment and finance. In one 2016 estimate, the CDB and Ex–Im Bank combined had more global assets deployed (around US$ 570 billion) than the World Bank and Asian Development Bank combined. China's Ex–Im Bank focuses on trade promotion through export credits, as well as on 'concessional', or low-interest, loans to poor or middle-income countries (mostly in Africa, the Caribbean and Asia). Such loans are often made as part of an overall package where the loan is bundled with infrastructure or other investments for Chinese firms and where payment is sometimes to be made through commodity trade deals. The CDB has staked out a rather different profile, mainly by providing financing (often for amounts that dwarf most Ex–Im Bank deals) for energy deals, mostly at near commercial rates, to oil or gas-rich countries in Latin America, Africa, Central Asia and to Russia.

From a mercantilist perspective, China's policy banks are often seen as agents of Chinese state-capitalism that employ subsidised capital to achieve a combination of commercial and geopolitical aims, while Chinese policy-makers claim that these banks simply serve to provide mutually beneficial 'development' opportunities for China and (often) its developing country partners. Without question, however, they are key tools in China's mixed, state-capitalist system and, as such, both policy banks receive privileged access to capital, which they deploy globally for a combination of diplomatic and commercial goals. Of the two, the Ex–Im Bank is less commercially focused, at least in terms of the low-interest loans it provides, but even its concessional loans are primarily made in the service of commerce, as they are frequently part of a 'package' where the loan is linked to investment and trade provisions.

Although China's policy banks have to date been most active in developing country regions such as Africa, Asia and Latin America, they are also increasingly playing a role in Europe and its periphery. So far, it is China's Ex–Im Bank that has played the most direct role both in and near the EU. Similar to many of its deals in Africa, Asia and the Caribbean, the Ex–Im Bank has focused on concessional,

package-deal lending for infrastructure projects in countries whose options for obtaining international financing are limited. Within the broader diplomatic construct of China's 16+1 framework for engagement with Central and Eastern European countries that are both inside and outside of the EU, China and its Ex–Im Bank have increasingly become active in infrastructure deals in the Western Balkans. The most well-known and controversial of these are upgrades and new construction of a 350-kilometre high-speed rail line in Hungary and Serbia, linking the two countries' capitals. While the details are still opaque, as is often the case with Chinese policy bank loans, the Ex–Im Bank is said to be providing a concessional loan to cover 85 per cent of the US$ 3 billion for the Hungarian portion of the project alone. Although the high-profile Chinese purchase of a controlling stake in Greece's Piraeus port was not financed by the Ex–Im Bank, Chinese officials claim that the Hungary–Serbia rail project is to be linked to Piraeus (via the Former Yugoslav Republic of Macedonia), all of which is framed under the umbrella of the BRI. But elsewhere in the Western Balkans, including in Montenegro, Bosnia and Herzegovina and Albania, China's Ex–Im Bank is financing motorways and physical infrastructure projects. Given that the Ex–Im Bank has largely specialised in concessional lending and export credit provisions to poorer countries that have few options for obtaining international finance, it is likely that its primary activities in Europe will in the near term remain focused on infrastructure financing in the Balkans and Eastern Europe. Yet in the medium to longer run, it is likely that China's Ex–Im Bank, and also the CDB, will seek more deal options inside the EU itself, including in finding joint-financing efforts for Eurasian 'connectivity' projects such as the BRI.

The Ex–Im Bank's involvement in infrastructure lending and construction in both EU and EU candidate countries in the Balkans and Eastern Europe underscores the direct role that Chinese policy banks are playing within and very near to the EU. Such involvement is important for the EU on a range of levels, including sovereign debt burdens, sustainability, and the impact on both procurement and construction standards for transportation infrastructure. Yet geographically further afield, both the Ex–Im Bank and the CDB are relevant for EU foreign policy. In Russia and Central Asia, the CDB has been a major player in financing multi-billion-dollar oil and gas deals among government-run firms. In Africa, the Ex–Im Bank is the key Chinese player in providing concessional loans for commodities and infrastructure deals, as well as providing export credits to Chinese firms there. In Latin America, especially in Venezuela, the CDB is the largest provider of sovereign debt and therefore increasingly linked to debt-repayment crises there (with knock-on effects in places like Curaçao). Last, but perhaps most importantly in the near to medium term, the CDB and Ex–Im Bank are already playing a major role in financing for BRI projects, both on their own and in other Chinese-backed financing vehicles such as the Silk Road Fund.

In their efforts to play a role in BRI financing, both banks are likely to seek European partners, including through joint funding vehicles like the one that the CDB signed with Deutsche Bank in 2017 and another under discussion with former UK Prime Minister David Cameron. Thus, even though the two main Chinese policy banks are not yet highly active in the heart of the EU itself, they are increasingly important on its periphery, are a core component of China's activist foreign policy in other parts of the world, and will certainly attempt to finance more projects within the EU and find co-financing opportunities with European counterparts. What this means for Chinese influence in Europe is that China's policy banks, despite the enormous resources that they are deploying on the global level, are primarily operating for now on the EU's periphery. It is here, especially within the 16+1 framework, that they are likely to play the most influential role in efforts to facilitate China's economic and broader diplomatic strategies.

Conclusions and Implications

China's policy banks and their role as providers of official Chinese international finance are important in their own right, but also because of what they can tell us about the controversies surrounding China's multifaceted foreign policy tool kit. China is increasingly referred to as the largest provider of global

development finance, with the CDB and Ex–Im Bank in the lead, yet only a minority of that is in the form of development 'aid', while most is targeted at the promotion of Chinese trade, investment, financial and infrastructure deals. These banks are increasingly employing lending models that they have created elsewhere in the world (often in developing countries) and implementing them in and near the EU itself. As official 'policy banks', it is clear that they see their role as fulfilling commercial and policy/diplomatic aims at the same time.

Yet the mercantilist-versus-Peaceful Development frameworks, as well as the hybrid conflict concept itself, are of relatively little value in understanding policy implications for the EU in light of the growing role of China's policy banks. Most mercantilist and Peaceful Development-type analyses miss, for instance, the possibility that Chinese financial and political risk analysis for the provision of finance through its policy banks is prone to mistakes because of inexperience and distorted economic and political incentives. Any given Chinese loan may therefore end up at high risk of default, thus putting both creditor and debtor (not to mention third parties such as the EU) into uncharted waters. Such unintended consequences, however, also pose an opportunity for creative diplomacy, especially in the realm of debt-default resolution, which in turn could allow the EU and China (and possibly the United States) into new discussions about how to include China in setting standards regarding best practices for the provision of infrastructure finance.

The following are some take-away implications of the foregoing analysis:

- China's policy banks are key institutions, deploying significant resources, in China's broader economic statecraft strategies. They pursue a mixture of commercial and policy aims, which from a Chinese perspective is a 'natural' part of the government's aim of making China a key agent and leader of global 'development'. In this way, China's policy banks serve to further China's commercial and geopolitical ambitions at the same time.

- Yet in recognising the dual commercial/geopolitical aims of China's policy banks, it is important for European officials to understand the aims themselves, as well as their potential appeal and flaws:
  - To argue that China's policy banks combine a mixture of commercial and policy aims mostly amounts to saying that China seeks to gain advantage for its own companies, including in the EU and its periphery.
  - The countries most likely to find broad appeal in doing deals with China's policy banks are those that otherwise have difficulty in accessing foreign finance and investment, and/or are keen to 'poke a finger' in the eye of larger, more dominant countries or regional institutions. In the Western hemisphere, Venezuela is a perfect example, whereas in the European context countries such as Hungary and Serbia have so far been most eager to work with the Ex–Im Bank in particular.
  - Simply because these policy banks have a combination of commercial/policy aims does not mean that they are always adept at achieving those aims. Ex–Im Bank infrastructure financing deals and CDB energy deals are often difficult to implement given that their partner countries are poorly governed, business partners are corrupt and that their own understanding of the local environment is incomplete at best. Especially in the context of the EU, similar to the United States, many countries will have strong resistance to state-to-state financing deals that involve taking on sovereign debt. It is also sometimes the case that the CDB and Ex–Im Bank compete with each other as much as they cooperate, and Europe may very well turn into a space for such competition.

- It is in the area of debt sustainability that EU policy-makers should not only be aware of Chinese dual commercial/geopolitical aims, but also of unexpected outcomes for both lenders and debtors. Especially in poorer or more poorly governed countries, taking on excessive sovereign debt for any given project with a Chinese policy bank may lead to default or exposure to Chinese economic, political or diplomatic leverage. It is not clear how the Chinese banks or foreign policy officials will react to such a situation in the European context, but the EU should both seek to understand better

the debt sustainability of any given Chinese policy bank deal in the EU or EU candidate countries and to have provisions in place in case of debt distress or default. This includes opening channels for discussion with China, possibly via the policy banks themselves, about debt sustainability in general and in relation to the BRI more specifically.

8 China's Political Influencing Efforts in Europe

Jan Weidenfeld (MERICS, Berlin)

Introduction

Political influencing has become an increasingly visible and consequential feature of China's engagement in EU member states and neighbourhood countries. While the global political influencing efforts of President Xi Jinping's China have received much less scrutiny than those of Vladimir Putin's Russia, Europe neglects Beijing's activities in this critical domain of hybrid warfare at its own peril. The Chinese Communist Party (CCP) commands a sophisticated set of influencing means, ranging from the overt to the covert. While some effects of China's political influencing efforts in Europe are already visible, their full impact – if unchecked – will only become tangible in the medium to long term. In countering China's political influencing efforts, European governments and Brussels should bolster intelligence activities, promote transparency and public awareness and take the 'China factor' more rigorously into account when approaching policy-making at European level.

Promoting Regime Stability at Home and China's Political and Economic Model Abroad

Part of a global effort, which has seen other liberal democracies such as Australia, Canada and the United States being targeted as well, China's efforts to exert political influence in Europe align with two principal motives of the CCP's policy-making: one defensive in nature; and the other offensive. First, all policy efforts pursued abroad, including political influencing, are expected ultimately to underpin regime stability at home. Second, in engaging with the rest of the world, Beijing is more convinced than ever that its approach to political and economic governance is not only highly competitive, but ultimately superior to that of liberal democracies.

Against the backdrop of these motives, political influencing efforts in Europe serve three, partly interrelated, strategic goals. First, political influencing efforts aim at silencing voices that are critical of the CCP and Chinese policies, such as Beijing's treatment of individual freedoms or minorities. Second, the CCP seeks to secure third-party legitimisation of and support for critical foreign policy projects and positions, such as its global infrastructure foreign policy, territorial claims in the South China Sea or the recognition of Market Economy Status. The third goal is more systemic in nature and consists of the popularisation of China's political and economic model with the rest of the world – including to thwart the expansion of liberal and democratic values and to diminish the appeal of Western soft power.

Deploying Wide-ranging Political Influencing Means in Europe

The mechanisms that the CCP employs in Europe to exert political influence range from economic carrot-and-stick tactics, through exploiting ideological proximities, to targeted investments into opinion-shaping entities. These mechanisms are primarily targeted at three groups, namely political and business elites, public opinion shapers and ultimately European publics at large. Rather than engaging in Kremlin-style short-term disruption techniques, which are geared to fostering public

distrust in liberal and democratic values at specific points in time, the CCP aims to build lasting stocks of influence in Europe, which are meant to help popularise the Chinese model over time.

On the back of the 2008 financial crisis, China has significantly stepped up its infrastructure financing and investments across Europe. While primarily aiming for economic gains, Beijing considers political dependencies and influence a valuable by-product of commercial activities. The CCP hence implicitly assumes that – over time, in many cases – money provided by state-led Chinese banks as well as state-owned enterprises to fill financing or investment gaps in EU member states and accession countries will result in 'receiving governments' political support' for Chinese positions and policies.

China also incentivises boardroom-level decision-makers from major European companies to lend their support to China's global infrastructure foreign policy, the BRI, with such support being a prerequisite for becoming an 'attractive' Western partner for Chinese investors and contractors in the realisation of BRI projects in third markets. Senior executives of companies such as DHL and Siemens have publicly echoed Chinese BRI marketing language and praised the CCP for its vision, including in Chinese state-media outlets. Notably both DHL and Siemens are key contractors on various BRI projects. Individual businesses and business associations at EU member-state level have also lobbied their respective national governments to adopt a positive stance towards BRI, negating any adverse geopolitical and macroeconomic effects of the initiative.

In a more 'traditional approach' to political influencing, the Chinese government has repeatedly engaged in episodes of freezing political and economic dialogues with individual EU member states, including Belgium, Denmark, Estonia, Germany, Lithuania, Slovakia and the United Kingdom, in response to these EU member states hosting the Dalai Lama. In freezing political relations, Beijing pursues a long-term strategy geared towards cultivating self-restraint among European governments when it comes to criticising China, the success of which has become visible in Norway, for example. Hence, after a prolonged period of frozen relations between Oslo and Beijing between 2010 and 2016 as a result of the Norwegian Nobel Committee awarding the 2010 Nobel Peace Prize to Liu Xiaobo, Norway's political elites have lately been rather cautious when issuing public statements on China and Chinese policies. For example, Norway's Prime Minister Erna Solberg refused to comment on calls for Liu Xiaobo's release in July 2017, as she reportedly did not want to put negotiations over a free-trade agreement with China at risk.

China also actively courts European political elites who display a certain degree of ideological proximity to Beijing and who refute liberalism and wider European values. Hungary's Prime Minister Viktor Orbán, who has openly advocated building an 'illiberal state on national foundations' is a prominent example. For example, in an October 2016 speech at the China–CEE Political Parties Dialogue in Budapest, Orbán endorsed Beijing's rejection of universal values and rights and supported the CCP argument that each country needs a system that fits its unique national conditions. This view contrasts strikingly with the EU's commitment to promoting human rights and is one that seems increasingly widely shared within Hungarian ministries. Significantly, illiberal and China-friendly rhetoric, comparable to that of Orbán, has also been put on public record by Czech President Miloš Zeman, as well as high-ranking politicians from NATO member Turkey and various EU membership candidate countries. In all of these countries, it is not only top level political decision-makers, but also a wider political class that view close ties with Beijing favourably.

Chinese efforts to build political capital and influence with political elites of a certain ideological proximity are by no means limited to Central and Eastern Europe (CEE). In Germany, for example, Chinese diplomats and journalists have been actively reaching out to politicians from the illiberal *Alternative für Deutschland* political party. In the run-up to the 2017 German federal elections, the fringe political party *Bürgerrechtsbewegung Solidarität*, whose leadership has established close ties with the CCP, adopted official Chinese political language for its campaign, including advertisements in central locations in Berlin claiming that "the Silk Road is the future of Germany!".

In another effort to influence European governments' positions on China and policy issues critical to the CCP, the Chinese leadership has started to leverage its personal ties with EU heads of state and government, as well as their staffs, to influence personnel decisions related to China policy. The Czech Republic has repeatedly served as an example of how China has used contacts at the top level of national administrations to ensure marginalisation of China-critical voices in those administrations. In spring 2017, for example, the Czech Ambassador to Beijing was severely criticised publicly by Czech President Zeman after he had signed a non-public human rights observance appeal addressed to the Chinese Public Security Minister along with ambassadors from other EU member states and like-minded countries. Zeman eventually 'punished' the Deputy Foreign Minister who had approved the co-signing of the appeal, refusing to confirm the diplomat's appointment as Czech Ambassador to the Organisation for Security and Cooperation in Europe.

However, China has not only induced Czech leaders to 'silence' critical voices, it has also taken steps to insert proponents of Chinese interests into the Czech administration. Hence, President Zeman officially appointed Ye Jianming, a Chinese citizen and former Chairman and Executive Director of Global Fortune 500 energy and finance conglomerate CEFC China Energy and a major investor in the Czech Republic, as a senior economic policy advisor. While Ye has lately fallen out of favour with the elites in Beijing and been subject to prosecution, evidence suggests that he has had strong ties with nationalistic elements of China's People's Liberation Army. Significantly, in providing economic advice to Zeman, Ye might also have had access to a vast array of confidential EU documents related to trade and investment, as well as other issues of interest to Beijing.

While the CCP has been less successful to date in 'gaining a foothold' in Western European administrations, it has been actively trying to 'cultivate' individuals close to political decision-making processes. Hence, a growing number of former top-level politicians from Western Europe are currently on China's payroll and expected to popularise Beijing's policies. In the most high-profile case, former British Prime Minister David Cameron took on a leadership role in a US$ 1 billion BRI infrastructure investment fund in December 2017. Similar types of roles have also been accepted by former prime ministers and ministers from France and Germany.

To gain influence over the way in which critical shapers of European opinion portray China, the CCP and Chinese media corporations have increasingly explored options to buy struggling media in Europe, which they consider as enjoying greater credibility with European audiences than Chinese media outlets operating in Europe, such as the *Global Times* or *China Global Television Network* (*CGTN*). Outside Europe, both party-state media and mainland Chinese corporations have made several attempts to buy major Western media institutions, including *Newsweek* magazine and *Forbes* magazine. Hong Kong's *South China Morning Post* was the first major medium successfully acquired by a Chinese investor. In late 2017, CEFC China Energy made a bid to buy Central European Media Enterprises, a media conglomerate operating primarily in Bulgaria, the Czech Republic, Romania and the Slovak Republic that has significant market share in all these countries.

To date, the most critical media channel by which China creates support among wider European publics for its interests and views is paid media inserts. The main element of this is *ChinaWatch*, an eight-page insert prepared by the *China Daily*, China's first and most important English-language daily since 2010. While *ChinaWatch* carries a disclaimer marking it as paid content, its layout makes it look like editorial content. At present, *ChinaWatch* is published by at least seven European newspapers in five languages: English; Spanish; Dutch; German; and French. In addition to supplements published at regular intervals in specific media, various Chinese actors also sometimes buy one-off advertising space in other media. Supplements such as *ChinaWatch* expose readers of the original publication to China's official point of view on various matters through the inserts. The fact that newspapers are paid to run *ChinaWatch* might also create dependencies and, by extension, the potential to influence content in the parent publication.

With a view to injecting Chinese viewpoints into European public debates, Beijing has recently also established Chinese think tanks in Hungary and Bulgaria. In addition, the Chinese Academy of Social Sciences (CASS) – the State Council's think tank – has created and financed a network with think tanks from sixteen CEE countries. Within the think-tank network, exchanges are mainly focused on gathering information about perceptions of and obstacles to Chinese initiatives in Europe. In the longer-term, these research exchanges have the potential to exert direct influence on future political elites of the countries involved, as the network's partners include universities and research institutes that train civil servants, as well as military and law-enforcement personnel.

A prime target of knowledge production and dissemination funded by the Chinese state has been the think-tank landscape in Brussels, with China's mission to the EU co-organising public events with established and highly visible local think tank partners. These tend to promote China's narratives on issues at stake in EU–China relations, such as debates concerning Market Economy Status, and by deploying Western voices that could look more credible to a European audience, alongside Chinese officials.

Beijing also increasingly aims to shape China-related curricula at European universities, funding academic programmes and trying to control academic debates through an established network of about 160 China state-funded Confucius Institutes and a wide-ranging network of Chinese Students and Scholars Associations (CSSA). Some Confucius Institutes in Europe have been shut down because of concerns over Chinese influence (for example, in Sweden, four out of five Confucius Institutes have been closed in recent years), and the nature of their presence at US universities has recently been a subject of concern among US decision-makers. Instances of CSSA members being deployed by the local Chinese embassy to control overseas Chinese students who take part in politically sensitive events or to lodge complaints against universities if the Chinese government is criticised during public debates took place at Durham University in the United Kingdom (in February 2017) and at Trinity College Dublin in Ireland (in 2014 and 2015).

Remaining Mindful of Potential Larger-scale Effects of China's Political Influencing Efforts in Europe

Some preliminary effects of China's political influencing efforts in relation to political elites have already become visible at the level of EU politics. In recent years, the EU has been significantly less able to act cohesively *vis-à-vis* China on trademarks of EU foreign policy, namely upholding the rule of law and protecting human rights. In July 2016, Hungary and Greece fought hard in Brussels to avoid a direct reference to Beijing in an EU statement about a binding international tribunal ruling that struck down China's legal claims over the South China Sea. In March 2017, Hungary derailed the EU's consensus to sign a joint letter denouncing the reported torture of detained lawyers in China. In June 2017, Greece blocked an EU statement at the UN Human Rights Council criticising China's human rights record, marking the first time that the EU failed to make a joint statement at the UN's top human rights body. The CCP's increasingly close ties to some European leaders might also mean that sensitive EU and national information might end up much faster in Chinese hands, facilitated by 'enablers' embedded in political processes at national and EU levels.

However, the full weight of implications of Chinese influencing actions, specifically regarding opinion-shapers and wider public opinion, might only become visible in the medium to long term. Chinese media supplements as well as future media acquisitions in Europe may not immediately result in changing European views on China and the issues about which the Chinese government cares. However, media takeovers and insertions will help the Chinese government to infuse more 'pro-China' talking points into European debates, without there necessarily being awareness among the wider public about their origin.

Chinese think tanks close to the CCP will also continue to expand their footprint in Europe. In doing so, they will aim to make a more active contribution to public debates, providing, for example, op-eds to newspapers in target countries with a 'Chinese perspective'. For European think tanks relying on Chinese funding, questions about the independence of research as well as event organisation will become more relevant. The incentives for Western scholars to cooperate with and accept financing from China will also remain high. Besides a lack of alternative funding sources, fear of losing access to Chinese officials (or the promise from the Chinese side to grant high-level access) will push many Western institutions to accept compromises in presenting their views, to adjust conference agendas in a way that is accepted by Beijing, and to change crucial terminology in publications.

As Chinese actors expand their investments in European universities in the years to come, there will be even more significant efforts to influence curricula, specifically as they relate to developments in China or events on topics that are politically sensitive to China. Beijing will also continue to use more traditional tools to foster self-censorship in European academic circles, such as preventing scholars from obtaining visas to travel to China if their views are not aligned with those of the Chinese government. Growing CCP control over Western campuses, including European ones, and internationally funded programmes in China might also result in a change in how China is discussed in European universities.

Bolstering Intelligence Activities, Promoting Transparency and Public Awareness and Taking the 'China Factor' More Rigorously Into Account

To pre-empt the medium- to long-term occurrence of any major unwanted effects of China's political influencing efforts in Europe, European governments should prioritise 1) bolstering intelligence activities, 2) promoting transparency and public awareness and 3) taking the 'China factor' more rigorously into account when approaching policy-making at EU-level.

National intelligence agencies should take a pro-active lead on initiating 'plausibility checks' for think tank and academic input feeding into policy-making processes that relate to China. They should also strengthen their efforts to raise awareness among stakeholders about Chinese influencing efforts, focussing on high-level decision-makers as well as powerful opinion-shapers. Last but not least, intelligence agencies should consider offering a mechanism to ethnic Chinese to blow the whistle and to receive help when they become subject to 'unwanted pressures' from the CCP.

Arguably, the most powerful strategy for countering China's political influencing in Europe is to be found in the public sphere by promoting transparency and public awareness. First and foremost, this requires encouraging greater funding of investigative journalism, think tanks and academia. Currently, European public knowledge of the different channels and effects of Chinese political influencing remains severely limited. Educating the public about – and hence making it less susceptible to – Chinese political influencing efforts in Europe can only succeed if there is sufficient impartial expertise on China. However, many European countries currently lack such expertise. A growing amount of China-related European research is China-sponsored, while high-quality journalism is suffering from rapid changes in the media landscape and corresponding budget cuts and an increasing number of journalists go through training programmes designed and funded by the CCP. Besides encouraging greater investments in high-quality China-related work of media, think tanks, and universities, European governments should also discuss the need to establish funding transparency requirements for these critical shapers of public opinion. Such transparency requirements should relate to funding received from any third country source, any lobbying on behalf of such a country, or provision of professional services for the furthering of third country interests.

In the future, many EU member states will also have to take the 'China factor' more rigorously into account when approaching policy-making at EU-level. As China's political influence in Europe is for now primarily a product of investments or promises of investment, the EU needs to continue to provide attractive counter-proposals. In doing so, it can leverage the fact that most investment within the EU and its periphery undoubtedly still comes from within Europe. However, the EU also needs to be aware that any reduction in structural funds for countries such as Hungary could result in a greater opening for China. On the back of its forthcoming EU-Asia connectivity strategy, the EU will need to set up mechanisms to align BRI investments in its neighborhood with European interests. This requires the European institutions and EU member states to pursue development policies that enable third countries to properly evaluate and monitor large-scale infrastructure projects, including those financed by China. It also means nudging Beijing towards channeling as much infrastructure investment as possible through multilateral frameworks, like the EU-China Connectivity Platform or the China-driven but largely Western-styled Asian Infrastructure Investment Bank (AIIB), and promoting co-financing models involving Chinese institutions and the EIB and EBRD. Last but not least, ongoing debates within various EU member states and in Brussels concerning the modification of national investment screening mechanisms and the introduction of such an EU-wide mechanism should go beyond traditional national security considerations. Instead, they should also put emphasis on the introduction or expansion of 'public interest' tests, for instance, where the acquisition of national media is concerned.

9 Chinese Direct Investment and Dutch National Security

Frans-Paul van der Putten (the Clingendael Institute, The Hague)

Introduction

The National Coordinator for Security and Counterterrorism of the Netherlands (known as NCTV) defines hybrid conflict as a conflict between states, largely below the legal threshold of open armed conflict, with the integrated use of means and actors, aimed at achieving certain strategic goals. Against this background, the following analysis focuses on Chinese direct investments and addresses three questions. First, is China making use of direct investments abroad in a coordinated way in order to achieve strategic goals? Second, if this is the case, to what extent does this represent a threat to Dutch national security? And third, how does this relate to the concept of hybrid conflict?

A major feature that distinguishes direct investments from other types of investment or other forms of economic interaction is the potential or actual change of managerial control. Direct investment is defined here as a transaction that gives the investor the ability to appoint at least one executive member of the company's board of directors.[22] If an investor controls the majority of voting rights within the board of directors, it has formal managerial control even if it does not own all shares in the relevant company.

China's Approach to Outward Direct Investments

The Chinese Communist Party (CCP) controls the Chinese state, while state-owned companies and state-owned financial institutions are responsible for a large part of Chinese direct investments abroad. Moreover, both the CCP and the state have a significant degree of influence over China's major private companies. The CCP not only has the capacity to exert influence over outward direct investments, but it also does so in a coordinated way. The Belt and Road Initiative (BRI, launched in 2013) is a policy framework that stimulates Chinese investors to contribute to the expansion of international networks of transport, energy and digital linkages. Another policy framework, Made in China 2025 (MC2025, launched in 2015), promotes Chinese investments in foreign assets that help China become a leading player in a range of advanced technologies, such as information and communication technologies (ICT), aerospace, robots, 'new energy' vehicles and medical equipment. An important outcome of these two initiatives, if they are successful, would be that China's dependence on external factors would be significantly reduced. Simultaneously, Chinese firms and financial institutions – and with these, the Chinese state and CCP – would have achieved an important degree of influence over global supply chains. This, in turn, would make foreign economies more dependent on China. Given the consistency and intensity with which China promotes and implements both initiatives, it seems clear that they are intended to improve China's competitive position in the global economy. In August 2017, the Chinese government promulgated policy guidelines to encourage outbound investments that, among other goals, facilitate the BRI and strengthen investment cooperation with foreign high-tech enterprises.

22 On the relevance of an investor's power to appoint top executives for assessing the impact of direct investments on national security, see Claartje Bulten *et al.*, 'Vitale vennootschappen in veilige handen', Nijmegen: Radboud Universiteit, February 2017, p. 49.

It is assumed that these favoured types of investment will obtain official support in fields such as regulatory procedures, tax, foreign exchange, insurance, customs and information.[23] The same guidelines also defined which categories of outbound investments are restricted or prohibited.

Improving international competitiveness is a common strategic aim for the foreign economic policies of countries around the world. What makes China special is the combination of the following three elements: 1) China is the second largest source of outward direct investments (behind the United States), accounting for US$ 245 billion in 2016;[24] 2) China's political leadership has a greater ability to coordinate outward direct investments than most countries; and 3) China's economic competitiveness is a major source of its global political influence. It therefore makes sense for host countries to pay special attention to direct investments from China, as they may have significant economic and political effects.

Some remarks are relevant to put the above in perspective. First, in the longer term the CCP and Chinese government are increasingly likely to control access to certain raw materials, technologies or trade routes, but present-day reality is that they already control foreign access to the Chinese economy, which is the second largest in the world and – most importantly – the largest contributor to global economic growth. China's outgoing investments may enhance its economic power, but they are not its primary source. For many countries, the fact that they need China as an export destination more than vice versa determines the (unbalanced) nature of the bilateral relationship. Second, the main agents of outward direct investments are not Chinese government agencies but companies. All companies, even major enterprises that are owned by the central government, have their own organisational interests and large companies themselves may have a certain degree of influence within the Chinese political system. For most individual instances of foreign direct investment, commercial motives are likely to play a leading role. Still, Chinese corporate investment strategies exist within frameworks that are defined by the government. Regardless of how these strategies are executed, the Chinese government and the CCP always have the possibility of exerting political pressure on Chinese investors to adjust or divest their foreign assets once they have been acquired.

Dutch Economic Security

China is still a minor source of direct investments in the Netherlands (responsible for approximately 1 per cent of overall stock by the end of 2015), but at the same time the rate of Chinese investments is increasing very quickly.[25] It is likely that the Chinese share in inward direct investments will continue to grow at a rapid pace. In terms of value, Chinese direct investments in the Netherlands are predominantly in mergers and acquisitions (M&A), rather than green field investments. Major M&A deals by Chinese investors include transactions in Dutch semiconductors (parts of NXP by JAC Capital), agribusiness (Nidera by COFCO), insurance (Vivat by Anbang), automotive (Nedschroef by Shanghai Electric and Inalfa by BAIC), and pharmaceuticals (part of DSM by Sinochem). A significant green field investor is Huawei, which is very active in the Dutch telecommunications sector. The majority of these mentioned investors are state-owned (with Anbang and Huawei being notable exceptions).

23 Buren Legal, 'China's New Policy on Outbound Investment', *China Law Special*, September 2017, https://www.burenlegal.com/sites/default/files/usercontent/content-files/Chinas%20new%20policy%20on%20outbound%20investment.pdf.

24 UNCTAD, *World Investment Report 2017*, Geneva: 2017, p. 14.

25 Frans-Paul van der Putten, 'Chinese Direct Investment in the Netherlands: Patterns, Reception and Political Significance', Clingendael Policy Brief, December 2017, p. 6.

The Dutch government has identified three types of risks with regard to potential negative effects on national security stemming from foreign direct investments:[26]

1. Strategic dependence – that is, an increased risk of political pressure on the Dutch government. This appears to be the most relevant risk. The Chinese government used its economic influence to apply pressure on the Netherlands on several occasions between 1980 and 1992 (in relation to the export of two submarines to Taiwan, and potential additional submarine sales) and again in 1997 (in retaliation for Dutch support for a proposed EU resolution to criticise China in the UN Commission on Human Rights).[27] Given ongoing differences between the two countries on values such as human rights, and increasing geopolitical tensions between China and the United States, an ally and close partner of the Netherlands, China will continue to retain an interest in options to influence Dutch policy-making on specific issues.[28] Chinese direct investments – which were virtually absent during the 1980s and 1990s – are not the cause for Dutch vulnerability in his context. However, they could further aggravate this type of risk, which relates to the possibility of investment withdrawal (from the Dutch economy) or of supply chain interruptions. Because of China's focus on global investments in key technologies and infrastructure, and the highly internationalised nature of the Dutch economy, the Netherlands is particularly sensitive to potential supply chain interruptions. This applies not only to supply chains that start or end in the Netherlands, but also to those in which Dutch-based companies or institutions play an intermediate role.

2. Disruptions to key infrastructure (so-called 'vital processes'), such as electricity, water supply, internet and basic financial services. In the absence of a direct military conflict between the Netherlands and China, it is unlikely that the Chinese government would be interested in causing disruptions to Dutch vital infrastructure. Moreover, under conditions of military conflict, cyberspace would probably provide ample vulnerabilities that do not require direct investment. Still, the possibility of Chinese investors withdrawing their involvement or services from Dutch vital infrastructure could add to a sense of strategic dependence.

3. Loss or compromise of strategic information, including state secrets, personal data, or information on national security processes. While the Dutch intelligence services are concerned about large-scale information theft by Chinese actors, this risk results primarily from intrusions via the internet and appears to be aimed most often at acquiring commercial and technological data.[29] Still, direct investments abroad could provide Chinese actors with additional access to personal data of Dutch citizens or – more rarely – information on national security processes.

While the risk of strategic dependence seems to be the most relevant of the three risk types, the question must be asked of how much direct investments add to China's longer-existing ability to exert pressure by limiting access to its market. The risk of strategic dependence is mainly based on exports to and direct investments in China. In the coming decades, Dutch dependence on exports to China and the presence of Dutch companies inside China may well diminish to some extent. As China evolves from a 'made in' to a 'created in' type of economy, its need for Dutch products, technology, brands and experience is likely to decline. Outward Chinese direct investments may compensate for this process,

26 Letter of Minister of Security and Justice G.A. van der Steur to the Netherlands House of Representatives, 2015–2016, 30821, 27, 4 January 2016, p. 2. Also NCTV, 'Tussen naiviteit en paranoia', April 2014, p. 17.

27 Frans-Paul van der Putten, 'Van Semi-kolonie naar economische wereldmacht: China's toepassing van diplomatieke en economische middelen in de betrekkingen met Nederland sinds het einde van de negentiende eeuw', in: J. Thomas Lindblad and Alicia Schrikker (eds), *Het Verre Gezicht: Politieke en culturele relaties tussen Nederland en Azië, Afrika en Amerika*, Franeker: Van Wijnen, 2011, pp. 381–383.

28 Frans-Paul van der Putten, 'China's randvoorwaarden', *Internationale Spectator*, no. 66/5, May 2012, pp. 229–230.

29 Robert Bas, 'AIVD waarschuwt voor spionage China', *NOS*, 15 April 2011, https://nos.nl/artikel/233316-aivd-waarschuwt-voor-spionage-china.html.

as they strengthen the ability of the Chinese government to inflict damage on the Dutch economy through targeted supply chain interruptions or relocations. Perhaps the most obvious example of the latter would be to redirect traffic in goods away from Rotterdam and Schiphol to non-Dutch ports and airports. The Dutch Ministry of Defence refers to the economic interest of the Netherlands in uninterrupted flows of goods and digital data as flow security.[30]

A further question is whether the three types of risks discussed above cover all potential vulnerabilities. The Dutch government identified these risk types from a national security perspective. Since the strategic aim underlying China's policies in the domain of outward investments seems primarily related to strengthening China's economic competitiveness and decreasing its exposure to external influences, perhaps the focus should not exclusively be directed on the risks of strategic dependence and loss of sensitive information. The weakening of Dutch economic competitiveness may have effects that go beyond the damage caused by strategic dependence and information loss. A coordinated and financially subsidised Chinese government strategy that results in the large-scale purchase by Chinese investors of key technologies and/or major companies in the Netherlands would constitute a significant risk to the Dutch economy's international competitiveness. Both advanced technologies and large firms tend to require sustained investments over a long time to develop and cannot easily be replaced. This is a fourth type of risk that could result in a substantial weakening of the Dutch economy and thereby undermine resilience to national security threats.

Direct Investment and Hybrid Conflict

Based on the NCTV's definition, hybrid conflict as a threat to national security is a sub-category of inter-state conflict. The term therefore applies to the role of Chinese direct investments in Sino–Dutch relations only to the extent that there exists a conflict between the two countries. Conflict is a broad term that can mean 'fight' but also 'discord of action'. The Netherlands and China maintain friendly and close diplomatic relations, which suggests that they do not perceive each other as immediate or fundamental security threats. At the same time, there are areas in which important interests and views of the two actors are opposed. These areas include: a) the legitimacy of liberal values as norms for international relations; b) economic competition; and c) geopolitical competition between the West and China, particularly in relation to the security role of the United States. The term 'hybrid conflict' applies to these domains rather than to the overall bilateral relationship, and only to the extent that either side is exerting influence on the other by using, in an integrated way, 'means and actors, aimed at achieving certain strategic goals'.

The ambiguous nature of Sino–Dutch relations – friendly and yet with opposed interests in key areas – means that it is difficult to establish whether the term 'hybrid conflict' is appropriate. Regardless of the terminology, the more important issue from a Dutch national security point of view is that Chinese direct investments – with all the benefits that they bring – also involve risks. In the short term, these risks do not add much to existing vulnerabilities resulting from cyber-attacks and the Dutch dependence on trade with and investment in China. In the longer run, the effects of China's outbound investments (both in the Netherlands and in third countries) may gain greater significance and could result in greater strategic dependence and weakened national economic competitiveness.

30 Dutch Ministry of Defence, 'Houvast in een onzekere wereld', 14 February 2017, p. 17.

Policy Recommendations

- Build capacity to monitor Chinese direct investments into the Netherlands and third countries, both at the national and the EU levels. Monitoring should also include relevant Chinese policies and actors and should take into account other aspects relevant to Chinese economic influence abroad, such as trade, portfolio investment, multilateral economic governance and technology cooperation.
- Focus on the linkage between Chinese outward direct investments and global supply chains (flow security) in order to assess the risk of strategic dependence.
- Add the long-term weakening of national economic competitiveness as a fourth type of risk when analysing the potential impact of Chinese direct investments to the existing framework of analysis for national security (which currently is based on three risk categories: strategic dependence; disruptions to key infrastructure; and loss or compromise of information).
- Develop a strategic vision on the Dutch–Chinese relationship that integrates both the positive aspects and the issues on which the two countries have opposing interests. This strategic vision should form the basis for a coherent set of policies to mitigate risks resulting from Chinese direct investments, both nationally and in cooperation with the EU and other actors.

About the authors

Keir Giles is a Senior Consulting Fellow with the Russia and Eurasia Programme at Chatham House in London, and also serves as Research Director for the Conflict Studies Research Centre, formerly part of the UK Ministry of Defence. His expertise centres on the Russian approach to information warfare, including the subdomain of cyber conflict.

Stefan Meister is Head of the Robert Bosch Center for Central and Eastern Europe, Russia and Central Asia at the German Council on Foreign Relations (DGAP). He previously worked as a Senior Policy Fellow at the European Council on Foreign Relations, the Organisation for Security and Cooperation in Europe and the Transatlantic Academy in Washington DC. His expertise includes Russian domestic, foreign and energy policy; the interrelationship between Russian domestic and foreign policy; Russia's policy towards its post-Soviet neighbours; EU–Russia relations; German–Russian relations; and post-Soviet conflicts, particularly in the South Caucasus.

Tony van der Togt is a Senior Research Fellow at the Clingendael Institute, working on EU/NATO–Russia relations, Dutch bilateral relations with Russia, Wider Europe and Greater Eurasia. He is temporarily on secondment from the Dutch Ministry of Foreign Affairs, where he held different positions, dealing with Russia, Eastern Europe and Central Asia. He also serves as a member of the core group of the EU–Russia expert network and has contributed to the 'Minsk dialogue' process in Belarus.

Sico van der Meer is a Research Fellow at the Clingendael Institute. His research focuses on non-conventional weapons such as WMD and cyber weapons from a strategic policy perspective. He also has a special interest in North Korea and relations between North and South Korea. In 2016 he was seconded for seven months to the Taskforce International Cyber Policies of the Netherlands Ministry of Foreign Affairs.

Namhoon Cho is a Senior Research Fellow at the Korean Institute for Defense Analyses (KIDA), where he mainly studies North Korean issues such as the North Korean military, economy and WMD strategies, as well as security environments and strategies in North-East Asia. Dr Cho served as Director of the Center for Security and Strategy at KIDA, as a Senior Policy Advisor to the Defense Minister at the South Korean Ministry of National Defense, and on various government committees.

Jenny Jun is a Ph.D. student in the Department of Political Science at Columbia University. Her current research interests include the bargaining model of war, the strategic dynamics of cyber conflict and security issues in East Asia. She was a cybersecurity consultant at Delta Risk LLC and has co-authored a CSIS report on North Korea's cyber operations. She has presented her work at the Brookings Institution, CSIS, and the School of International and Public Affairs (SIPA) at Columbia University, and has provided multiple private briefings and media interviews on the topic.

Matt Ferchen is a non-resident scholar at the Carnegie–Tsinghua Center for Global Policy, where he runs the China and the Developing World Program. Ferchen was also a faculty member in the Department of International Relations at Tsinghua University. His research focuses on the political economy of the 'China model' of development, China's relations with Latin America, the nexus between development and security in China's foreign policy, and how China is managing political risk in its ties to fragile states.

Jan Weidenfeld is Head of the European China Policy Unit at the Mercator Institute for China Studies (MERICS) in Berlin. His research focuses on Europe–China relations as well as China's global security policy and infrastructure foreign policy. He previously worked at the RAND Corporation, the NATO Parliamentary Assembly, the EU Delegation in Vienna, the EU Institute for Security Studies and the European Centre for Development Policy Management.

Frans-Paul van der Putten is a Senior Research fellow at the Clingendael Institute, where he is a member of the Security Research Unit. His work relates to the geopolitical significance of China's growing international role. He previously worked as a researcher at the European Institute for Business Ethics at Nyenrode Business University and served as former editor-in-chief of *Itinerario – Journal on the History of European Expansion and Global Interaction*. He currently acts as coordinator of the editorial team of *Silk Road Headlines*, a weekly news digest on China's Belt and Road initiative.

Minke Meijnders is Research Fellow at the Clingendael Institute. In the field of international security issues, she focuses primarily on economic security. In addition, she is frequently involved in forecasting studies like scenario and trend analyses.