LUDVIG HAMBRAEUS

The American Response to Chinese Expansionism in Cyberspace

– U.S. Policy Deconstructed for a European Audience

LUDVIG HAMBRAEUS

The American Response to Chinese Expansionism in Cyberspace

– U.S. Policy Deconstructed for a European Audience

PUBLISHED BY EUROPEAN LIBERAL FORUM

European Liberal Forum asbl,
Rue d'Idalie 11-13, boite 6, 1050 Brussels, Belgium
info@liberalforum.eu
www.liberalforum.se

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 46 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard.

Centre Party
Stora Nygatan 4
Box 2200,
103 15 Stockholm, Sweden
info@centerpartiet.se
www.centerpartiet.se

ISBN 978-2-39067-000-1

LUDVIG HAMBRAEUS
The American Response to Chinese Expansionism in Cyberspace
– U.S. Policy Deconstructed for a European Audience

Cover & Graphic design: Mobile Design, Sweden
Printed by Stocken, Sollentuna, Sweden 2021

Published by the European Liberal Forum in cooperation with Centre Party International Foundation. Co-funded by the European Parliament. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum.

Content

Introductory Remarks

Chinese expansionism in cyberspace is a tangible reality of our day and age which actualises the need for a deeper understanding of both Chinese grand- and cyber-strategy, as well as a more holistic insight into how to best tailor a subsequent response.

U.S. private equity extraordinaire Stephen Schwartzman outlined it well: "In the 21st Century, China is no longer an elective, it is core curriculum". The same is true for European stakeholders and policymakers, whose understanding of and appreciation for Chinese cyber expansionism in many cases are directly attributable to the success of policies implemented under their supervision.

As we further the discussion on the wider implications of the U.S.-China relationship and its implications on European cyber policy, we must first outline the need from the European side to try and understand how U.S. policy and decisionmakers formulate their analysis of Chinese expansionism, and how they in turn are likely to attempt countermeasures against the former's expansionist tendencies in cyberspace.

In the following chapters, the reader should be able to gather a baseline understanding of Chinese expansionism in cyberspace and, the subsequent U.S. response, and finally how European decision makers can utilise their knowledge of these constructs when developing area-specific policy.

1

Defining 21st Century War and Diplomacy – At the Frontlines of Protecting Individual Rights and Freedoms in Cyberspace

Historical analogies

To understand how cyber capabilities inherently shape states' actions in terms of maintaining national defence and security, there first needs to be a baseline for how cyber fits into existing paradigms of diplomacy as well as military and grand strategy.

In this regard, contemporary strategists often think about a nation's cyber capabilities as the potentially decisive factor in a modern conflict between two belligerents (Richards, 2014: 15). One reason for this, as laid out in Wang (1999), *Unrestricted Warfare,* is the inherent power of cyber to outmanoeuvre conventional weapons and tactics and operate outside of the traditional military spectrum. By doing so, traditionally weaker states can inflict great damage on otherwise impenetrable national defences.

Despite inhabiting a non-physical realm, conflict in cyberspace shares plenty of analogous features with its traditional counterparts. Much like the Kaldorian theory of New Wars and the slow decimation of the nation-state, developments in cyber warfare challenges the significance and perceived strength of the Westphalian model of state-centric power by introducing new means by which weaker nations can deal considerable damage to stronger opponents by relying on asymmetric warfare and irregular military activity (Richards, 2014: 15). This increased potential for attacks on faraway foes, as we will come back to later, is one of the key factors as to why expansionism in cyberspace can threaten the lives and freedoms of people in uniquely far-reaching manners.

The lessons learned by western powers in general – and the U.S. in particular – from contemporary scrabbles in cyberspace adds to the overall theory of post-Cold War conflicts, in which one has had to adapt to a shifting conflict paradigm in order to retain tactical superiority, even if doing so meant stepping away from traditionally accepted strategic theories and challenge preconceived notions and dogmas.

Where we are Today

Cyber fits right into this new reality by blending conventional and non-conventional threats as well as novel methods of expanding ones' sphere of influence, creating a means of perpetuating conflict that is high in both complexity and attainability. However, despite these features, conflicts in cyberspace should be understood as an extension of advancement in the field of technology and the concept of RMA or Revolution in Military Affairs (Richards, 2014: 16).

As such, cyber warfare hails from the same fora of technological advancement that gave us UAVs, nuclear submarines, and drones. Seen from this perspective, the tools and tactics of cyber conflict can be understood not as existing in a vacuum but adjoined to technological advancement in general. The major difference being that conflicts in cyberspace often bridges the gap between state and private actors, military and non-military targets, as well as blur the legal definition of acts of war (Richards, 2014: 16).

Legendary military strategist Clausewitz once said that war is the continuation of politics by other means (Clausewitz, 1984: 87). That statement is as relevant today as it has ever been. The weaponization of states' and international organisations' cyber capabilities blur the line between war and peace, the classification of actors difficult, and opens a novel forum for remote attacks on infrastructure and civil

society that previously has been unthinkable. Understanding and adapting to current and emerging challenges in cyberspace is therefore not only important for global superpowers boosting multi-billion-dollar defence budgets, like the U.S. and China, but in fact equally – if not more – critical for states with less diplomatic swagger and a more modest voice in the regulatory processes of military affairs.

Furthermore, the inclusion of network-based features in many institutions of importance for the civil society additionally invokes the attention of non-military stakeholders and decision makers to think as though they were part of the national defence structure in a whole new way. Awareness of the fact that the weaponization of cyber capabilities in many ways has brought interstate conflicts into the server rooms and offices of public authorities, courts, power plants, as well as private businesses cannot be overstated in its importance.

Thus, for the purpose of this publication we can derive that Chinese expansionism in cyberspace usually takes on the form of a collective of more-or-less grey-zone offensive activities and tactics aimed to attack, infiltrate, or otherwise weaken one or more features of another state's military and/or civil infrastructure. These activities are hard to classify as they oftentimes involve actors belonging to regular civil society and target civilian institutions, like intellectual property or financial information. This was recently on display in the spring of 2020, when concerns were raised in the United Kingdom over the political agenda attached to Huawei's planned 5G expansion in the country (Bowler, 2020).

2

Chinese Theories of Defence and Security – Understanding Her Military Use of Cyber

The Chinese thinking on matters of defence and security has in years past been radically different from the traditional Western understanding. To this end, many confrontations can be interpreted as a result of American-Sino cultural shock.

Traditionally, the first common misconception was usually that Beijing strived to reinstitute a Sino-centric order in both the East Asia region and the world (Xinbo, 2000: 480). Allusions to this end was often used to motivate strategic actions against Chinese interests under the guise of political preparatory self-defence. This notion that China was – and in the eyes of some commentators still is – set on a similar trajectory to that of Putin's Russia is, however, wrong. First and foremost because of the fact that traditional Chinese thinking is grounded in establishing geopolitical power through multi-polarization – rather than through uni-polarization – and second of all because Beijing's endgame might not be the reassertion of old dominions or the reclamation of supposedly lost glory, but rather a somewhat measured response to events within its global dyad with Washington, where peace is seen to best be sought out by balancing regional power (Xinbo, 2000: 480).

Another traditional misconception on part of western decision makers is viewing Chinese efforts to strengthen their standing regionally as an attempt to eventually eclipse the United States in East Asia and eventually abolish any American influence in the region. This was never entirely true neither. Prevailing views of the U.S. among Chinese decision makers was traditionally one where Washington was seen as a natural player in the region rather than an invading force (Xinbo, 2000: 480).

The Chinese understanding of security was steadfastly rooted in the belief that mutual security trumps a unilateral ditto. Which implied that overconfidence in securitization through unilateral action was considered likely to bring increased unrest whereas responsible statecraft on the other hand would dictate the promotion of mutual and common security. The culmination of this argument crystalized in the cross-section where the American notions of absolute security met the above-mentioned notion of bilateral strength through the increase in mutual security. This cultural shock in diplomatic relations leaves both parties at a virtual standstill as their respective preferred positions are entirely non-compatible (Xinbo, 2000: 481).

After seemingly having adhered quite strongly to the above-mentioned notion in the recent past, China under Xi Jinping has seemingly adopted a less reactive and more activist cyber policy. One that on the external plane aims to shape cyberspace to extend Beijing's political and military influence and counter other states' – especially American – advantages in cyberspace (Segal, 2017: 1).

It is not China alone, however, who is responsible for the increased tensions in bilateral relations. Wu Xinbo argues that the most notable development impacting Asia-Pacific regional security in the year 2019 was the intensifying strategic competition between the U.S. and China (Xinbo, 2020). This increased tension was very much a result of the Trump administration's trade war with China, to which Beijing has opted to respond in kind. The trade war did not only increase competition, but it spilled over into the overall bilateral relationship (Xinbo, 2020), affecting other areas of interest like maritime security, cyber policy, and regional cooperation.

Faced with this increasingly strategic competition, Beijing has responded by undertaking a series of measures aimed towards diluting and offsetting U.S. actions in the region. This had led to closer ties between

Beijing and Moscow on security policy, a joint effort towards an integrated missile early warning system, as well as increased diplomatic efforts with ASEAN members of the code of conduct in the South China sea (Xinbo, 2020).

It can be said, therefore, that while some of the traditional approaches to Beijing's relationship with Washington persists – the Asia-Pacific region has entered a period of profound change spurred on by shifts in regional power and adjustments in grand strategy. The further the overall bilateral relationship between the U.S. and China is strained, the likelier it becomes that tensions might spill over and set of a serious crisis (Xinbo, 2020).

3

Intellectual Property Protection: Europe, the U.S. and the Chinese challenge – Understanding Her Non-Military Use of Cyber

Katarina Tracz *is the Director of Stockholm Free World Forum (Frivärld). She possesses wide experience in foreign and security policy analysis, focusing particularly on Transatlantic affairs and European security . She is an active contributor to the debate on foreign and security policy in Swedish and international media, and has published several reports, articles and OP-EDs in major Swedish and international newspapers. Tracz has previously worked as an International Research Fellow at the McCain Institute for International Leadership in Washington D.C. and has been a Marshall Memorial Fellow at the German Marshall Fund of the United States. Katarina is the author of the book "The Sea of Peace? Increased Tensions Around the Baltic Sea".*

China's economic development is unprecedented in history. Since the country opened up in 1978, Chinas economy has grown immensely. During the past four decades, the Chinese GDP has grown from less than 150 billion USD to 14.343 trillion USD in 2019 (The World Bank, 2020). Simultaneously, hundreds of millions of Chinese have left extreme poverty.

China is a country with clear strategic goals. The country's tremendous economic rise has been accompanied with growing ambitions in other areas. The ruling Chinese Communist Party has clear geopolitical ambitions which are often tied to the economic and industrial status of China.

In 2015, China's Prime Minister Li Keqiang launched *"Made in China 2025"* (MIC 2025). The initiative is a 10-year strategy aiming to moder-

nize China's industrial capabilities. This strategy evolves around 10 strategic sectors aiming at guaranteeing China's position as a global powerhouse in high-tech industries (Institute for Security and Development Policy, 2018).

The tactics to obtain the goals of MIC 2025 evolve around increased government control of key industries. As part of this, private and state-owned Chinese firms are encouraged to invest in foreign companies in order to access foreign intellectual property (IP). This has made several countries consider China's efforts under MIC 2025 as a security problem (Capaccio, 2018)

In 2018, U.S. intelligence officials stated that China's recruitment of citizens educated or employed in the United States constitutes theft of American intellectual property. U.S. intelligence agencies pointed out that China is working to facilitate "legal as well as illicit transfer of U.S. IP and technological know-how" to China (The National Bureau of Asian Research, 2017). In combination with targeted acquisition of U.S. firms, the agencies stated that China's actions constitute an "unprecedented threat".

When the Chinese state does not manage to obtain foreign IP though recruitment or acquisitions of foreign firms, it has been accused of sponsoring IP theft by means of economic espionage or cyberhacking.

Chinese theft of intellectual property has been estimated to cost the United States between 225 billion to 600 billion USD a year (Lee-Makiyama, 2018). The same pattern can be noticed in Europe.

An assessment made by the European Centre for International Political Economy (ECIPE) in 2017 shows that cyber espionage costs the European Union up to €60 billion annually. Accordingly, this

loss of economic growth put 289 000 jobs at stake. As the digital race accelerates, by 2025 the loss of European jobs due to cyber theft is estimated to reach up one million (Council on Foreign Relations, 2020). The Council on Foreign Relations (CFR) has monitored advanced persistent threat (APT) groups and incidents targeting EU interests. According to Cyber Operations Tracker, China is attributed as the state sponsor behind the actions in 8 out of 12 cases (Council on Foreign Relations, 2020), (Lee-Makiyama, 2018).

Consequently, loss of intellectual property, through cyber theft or by other means, is a central threat to the future competitiveness, development, and wealth of the American as well as the European society.

In the U.S., protection of intellectual property is an increasingly important political issue. In 2015, American President Barack Obama and his Chinese counterpart Xi Jinping expressed that they had reached a "common understanding" against economic cyber espionage. During the press conference where the statement was announced, Obama mentioned that he, in his discussions with Xi, had "raised, once again, our very serious concerns about growing cyber threats… I indicated that it has to stop." (Pepitone, 2015).

Since then, intellectual property issues have become a top political priority in the United States. Under the Trump administration, the United States has pushed hard for protection of American IP as part of the trade negotiations with China. For the United States, one of the key components of the "phase one" of the trade agreement with China has been the protection of intellectual property and against forced technology transfer (Pramuk, 2020).

Like the United States, the EU recognizes the problem. In its biennial report on the protection and enforcement of intellectual property

rights in third countries, the EU Commission presents a list of the union's trading partners ranked according to how well or poorly they are enforcing IP protection. In the last report, published in January 2020, China is labelled as Europe's "priority one" worst offender, due to the scope and perseverance of its policies, practices and negligence regarding IP protection issues (European Commission Staff Working Document, 2020).

During the Trump presidency, the Transatlantic relation has suffered in several ways. The rift between the continents has been especially noteworthy in security matters, manifested through Trump's vocal attacks on European NATO allies, and in matters of trade. An additional way in which the Transatlantic partnership has been hurt is by the de facto lack of cooperation in matters where the United States and Europe share common interests, such as the protection of IP.

The focus on China's actions regarding in cyber enabled IP theft is likely to continue under the Biden administration. The EU and the U.S. should seize this opportunity and work together in order to create a common approach. A joint U.S.- EU framework of standards regarding IP theft and forced technology transfer would have significant impact on third parties.

Together, the United States and Europe represent two of the three largest economies in the world. Moreover, both are facing an urgent security threat posed by economic espionage and cyber theft of IP, not seldom sponsored by the third of world's economic giants, China. A common Euro-American stance on IP protection would set the framework for constructive future trade cooperation with China. In addition, it would be an important step in assuring continued competitiveness, development, and wealth on both sides of the Atlantic.

4

The U.S. Response – Looking to Those Who Came Before

Much like the case with foreign policy as a whole, the tendencies in Washington to become increasingly inward-looking with each year of the Trump administration has indeed created opportunities for China to play a larger role in defining the rules of the international order in cyberspace (Segal, 2017: 2).

The Trump administration's cybersecurity executive order stated indeed that it is the goal of U.S. policy to promote an open, interoperable, reliable, and secure internet. The abandoning of bi- and unilateral agreements and weakening of alliance relationships has, however, weakened Washington's position to pursue its goals toward these ends.

The Trump administration was always very unlikely to become a vocal critic of China's domestic control of its internet. A likely result of the administration's *transactional nationalism foreign policy* ideology, U.S. diplomatic interactions with China in this area seem to circle around the notion of protecting American interests over promoting American values. Effectively, this has meant that the Trump administration has not carried forward the virtues of a free and open internet vis-a-vis China on the public diplomacy plane (Segal, 2017: 2).

Drawing a comparison from general U.S. foreign policy in this era, where the current administration has prioritized fighting extremists over criticizing the domestic policy choices of other countries, it is not unthinkable that this relative pragmatism will come to dominate U.S. cyber policy as well (Segal, 2017: 18). A recent example of this trend would be the Trump administration's unwillingness to condemn the Chinese government's violence towards the country's Uighur population.

However, a continuous response – or perceived lack thereof – like this could according to some scholars potentially lead to greater cooperation between the two nations. As an example of this line of thinking, the agreement struck between the U.S. and China under the Obama administration cracking down on commercial cyber espionage seems to still be holding water. This might indeed be simply a result of refined tactics, but the fact remains that a FiveEye report on the issue held that espionage activities relating to provisions under the agreement had taken a downturn following it coming into force (Segal, 2017: 18). Nevertheless, the response might also lead to the United States having to react to entirely new threats as Chinese cyber strategy morphs into increasingly utilizing covert attacks and shaping cyberspace through primarily commercial tools, in lieu of striking a static diplomatic tone on the issue.

The U.S. response then, going forward, can be expected to be two-fold. On the one hand, it is reasonable to expect U.S. public diplomacy to remain slightly vague. Albeit that any incoming administration might strike a new, harsher, tone. On the other hand, it is not unreasonable to expect contentions to continue beneath the surface. Indeed, already in 2015, multiple leading U.S. China experts voiced concern over what they perceived to be a deterioration in bilateral ties between the two nations. In doing so, they highlighted the need for a revised U.S. grand strategy toward China as a means to counter the latter's rising power in influence (Van der Meer et. al., 2015: 1). Conversely, Chinese scholars have argued for the U.S. and China to come together and regulate conflicts emanating in cyberspace as the lack of functional dialogue is reducing the room for cooperation on cybersecurity issues (Van der Meer et. al., 2015: 5).

Overt Response

In the spirit of limiting the damage of China's cyber capabilities and urged on by scholars and practitioners on both sides of the Pacific, it seems likely that an incoming post-Trump administration would like to take the opportunity and stake out a new public diplomacy route for the U.S. in relation to Chinese expansionism in the overt realms of cyberspace.

☆ *Diplomatic protest*

– Being largely symbolic, and inferring almost no risk for escalation, a diplomatic protest is a traditional – yet potentially quite potent – means of responding to an unwarranted action by another state. Actions like the expulsion of diplomatic personnel, while highly visible and potentially harmful from a goodwill perspective, can not only be mirrored by China but are also unlikely to embody the role of deterrent that is sought after (Van der Meer et. al., 2015: 4).

☆ *Economic sanctions and legal measures*

– Whilst being theoretically effective against export-dependent nations like China, the Trump administration's trade war has shown the relative futility of such actions within the scope of the U.S.-China dyad if their intended goal is to achieve Chinese adherence to a particular policy or norm.

– In 2014, five officers of the Chinese People's Liberation Army were indicted on charges of theft of intellectual property by ways of cyber espionage against U.S.-based companies. Again, however, both domestic U.S. law and international law – when applicable – has its limits in terms of enforceability. Hence, legal measures often join the ranks of the diplomatic protest in terms of effect (Van der Meer et. al., 2015: 4).

Covert Response

In lieu of public diplomacy – and diplomacy altogether for that matter – the United States is very likely to also deploy measures designed to more forcefully meet the kind of Chinese expansionism in cyberspace that cannot be met via diplomatic channels.

☆ *Retaliation in cyberspace*

– Threatening de facto retaliation has in the past proven to be a somewhat reliable deterrent. By manning a response against China in cyberspace, the U.S. would showcase that it does not tolerate attacks and that such undertakings come with serious consequences for the aggressors (Van der Meer et. al., 2015: 4). A retaliation in cyberspace could be undertaken with the goal to try to attain and publish sensitive information from the Chinese government or to paralyze key functions of the Chinese government apparatus (Van der Meer et. al., 2015: 5).

☆ *Military retaliation*

– Whilst a conventional military retaliation is all but unconceivable, it is still worth discussing here. To illustrate, a recent analogy could be made to the Trump administration's targeted strike on January 3rd, 2020, that hit and killed the Iranian major general Qasem Soleimani while he was visiting near the Baghdad International Airport, Iraq. The strike was defended by U.S. officials as necessary in order to prevent an imminent attack, a right drawn from an interpretation of article 51 of the United Nation Charter that is not commonly shared and accepted by all states privy to the Charter. The strike increased tensions, not only bilaterally between the belligerents, but in the region as a whole. This option for responding to Chinese aggression and expansionism in cyberspace thus seems highly unlikely, but should nevertheless be mentioned as an improbable yet possible response to a large-scale and destructive Chinese cyber attack (Van der Meer et.al., 2015: 5).

Consequences of U.S. Response and Retaliation

A U.S. response to Chinese expansionism in cyberspace would likely come with both drawbacks in rewards in the short term as well as the long term.

In the short term, it is likely that such measures from the United States would lead China to counterattack, risking further destabilization of U.S.-Sino diplomatic relations. Taking into account that the bilateral relationship in question already holds several points of contest – like control of maritime zones in the South China Sea and political decorum in relation to the One China policy – a conflict beginning in cyberspace comes with no guarantees of remaining there (Van der Meer et. al., 2015: 5).

As far as for the value of response and retaliation in the long term, Washington is likely to weigh the risk of escalation against the value of a successfully implemented deterrent when considering retaliatory actions against Chinese expansionism in cyberspace (Van der Meer et. al., 2015: 6). With this precarious balance in mind, the most likely course of action would probably be to respond to such acts in kind, meaning that Washington would prefer a covert cyber attack over any form of overt action (Van der Meer et. al., 2015: 6).

The fact that the United States – arguably being the global leader in cyber prowess – is finding it hard to find an acceptable form of response to Chinese expansionism in cyberspace shows us not only how the novelty and complexity of the subject demands more research and preparatory work, but also how difficult similar decisions are to smaller, less powerful, states (Van der Meer et. al., 2015: 6).

5

Lessons for Europe

All in all, the lack of a – at least publicly available – coherent and all-encompassing U.S. strategy for responding to Chinese expansionism in cyberspace does speak volumes about the complexity of the topic. Countries that in many ways depend on the U.S. to aid them in their own pursuit of national security should urge Washington at an early stage to refrain from seeking cyber deterrence through retaliatory action whilst the U.S. itself pursues their own similar goals. This is because of the fact that any escalation in that bilateral relationship could be seen as precedence for opening up the floodgates for China to strike against U.S. allies, thus further risking the infringement by Chinese actors upon our values and freedoms.

Preferably, U.S. allies should strive to work with the United States on a regular basis towards establishing norms and rules that may halt the proliferation of state-sponsored cyber expansionism and aggression (Van der Meer et. al., 2015: 6). This form of cooperation would not only be a net positive for the demystification of the area of cyber on a whole, but it would also be a great opportunity for U.S. allies in Europe to be a part of creating the framework of rules and regulation that eventually will come to envelop conflict in cyberspace.

In its official material, *EU-China: a strategic outlook,* the EU argues that it considers China as an economic competitor in the pursuit of technological leadership, next to being a negotiating partner and systemic rival. While Washington throughout the current administration's tenure has opted for strengthening its barriers against China and increasing the level of complexity and uncertainty of their bilateral relationship, Brussels has sprung for a more constructive dialogue.

This is not a naïve development, the cited report argues, but instead a sign that the European Union has started to adapt itself to a changed

global environment. Developing a more rules-based and reciprocal partnership with its Chinese is, as previously stated in this piece, desirable for several reasons. However, in going down this road it should be noted that China and the EU have very different approaches towards what constitutes good governance of cyberspace.

The EU supports a model comprising several stakeholders, including private actors as well as governmental ones, that should apply their labour towards creating and maintaining an open cyberspace, free from aggressions and intrusions (European Commission and HR/VP, 2019). This model is underpinned by the pursuit of individual rights and freedoms to lead the way for developing legislation around the internet and how we as individuals interact with it. In this model, the state only takes the role of facilitator in the development of regulatory instruments, thus anchoring any long-term changes in the democratically channelled will of the people.

China, on the other hand, bases their policy on a state-centric model wherein the notion of a singular source of control and superiority – exempt from external scrutiny and interference – is to be constructed. It is here that we should be weary of letting Chinese interests as well as our own self-interest in reaching a purely non-antagonistic diplomatic solution lead us astray. Too much cooperation between the EU and China might well lead to an increase in the types of limitations on rights and freedoms that such a diplomatic approach originally sought to motivate.

To exemplify this, it is useful to take a look at the effect China has had on the global human rights system. For some time, it was the goal of western democracies to get China to engage more in the global human rights system. In becoming more engaged at the UN, however, Beijing is now trying to rewrite norms and procedures to not only minimize the global community's scrutiny of its own government, but also to achieve the same alteration for all governments (Richardson, 2020).

This development is highly worrying for obvious reasons. However, taken together with increased Chinese direct influence over western democracies – through major investment in infrastructure, higher education, and popular culture for example – Beijing's reach and impact is a major concern for the protection of individual rights and freedoms in Europe and the world.

Reverting back to what was determined in chapter 2 of this piece, regarding fundamental differences between traditional Western thinking and the Chinese ditto, it seems to be the case that regionally and culturally related differences between how Beijing and its Western counterparts see the future of not only diplomatic and military relations, but also cyber policy and rights and freedoms online very much is a problem in its own right. If the EU is to successfully negotiate any form of agreement that covers the protection of a free and open internet void of malignant attempts at expanding Beijing's influence through either overt or covert means, the agreement in question must be one that also clearly stipulates the liberal values currently central to how the EU operates and manages to bridge the gap the two sides fundamental differences in thinking. Without creating a solid practical and theoretical foundation upon which a framework for protecting both European military and non-military assets and interests can be built, upholding the EU model for how to regulate cyber activities would appear to be an even taller order than it already is.

What conclusions can be drawn from this?

Firstly, that the problem of Chinese expansionism in cyberspace can most likely be satisfyingly resolved in the long-term only through diplomatic means. In the short-term, it is seemingly possible for a state with the military resources of the current United States to thwart cyber attacks on military and civilian targets to a somewhat satisfying degree. However, experts and scholars seemingly argue the point that

an escalation – purely in cyberspace, by more traditional means, or mixed – will have a devastating effect for both military and civilian assets in the country attacked. For states boosting militaries with less impressive cyber capabilities than the United States, any fallout from retaliation would consequently be much worse to contain (inter alia, Van der Meer et. al., 2015).

Secondly, that European stakeholders and policymakers need to think about how to approach this issue in terms of diplomacy. Initially, it would seem as though any attempts to reach a diplomatic solution would have to be based on a mutual understanding of the issue at hand and the values each side seeks to promote and protect. Such non-confrontative approaches has previously rendered some success. Most notably so in the case of the Obama-era U.S.-China Espionage Deal. Nevertheless, in lieu of being able to muster an overwhelming cyber response to Beijing, any diplomatic solution that the EU wishes to promote needs to emerge from a place of mutual understanding – not mutual destruction – if it aims to last.

As such, the first step that should be taken towards this goal is to attempt the establishment of a common understanding. For proof of concept, the EU can look to the U.S. and its previously mentioned Obama-era agreement with Beijing that has indeed helped make the internet a more secure domain for the persons and entities protected by the agreement through the establishment of joint goals and a shared understanding.

Finally, there is no denying China's rise as a global superpower – not to mention its ascension to the level of cyberspace powerhouse. Nevertheless, it falls onto the European Union to guard the interests of its citizens and countering any incursion on their individual rights and freedoms caused by Chinese expansionism in cyberspace.

6

Policy recommendations

In the light of the above mentioned, this publication would like to suggest that the following aspects are considered when approaching the notion of European cyber policy and Chinese expansionism in cyberspace.

The piece argues that:

1. The European Union should attempt to reach a long-term agreement with the People's Republic of China, wherein it is sought to establish a shared baseline and joint understanding of the liberal values as they adhere to a free, open, and secure internet and the importance of these values to the EU and its citizens. These attempts must, however, include notions of mutual appreciation between the parties on what the definitions of human rights are and the importance of protecting individual rights and freedoms as they are portrayed in European Convention Law.

2. Where possible, the European Union should strive towards closer cooperation and steadfast agreements – like NAFTA – with the United States on the issue of Chinese expansionism in cyberspace. This cooperation should focus on the importance of a free, open, and secure internet and its role in safeguarding and enabling an equally free, open, and secure market for the commerce of ideas, goods, and services between our unions. In the past, a strong Transatlantic bond has been the beacon of light that has helped guide policies promoting liberal values on both sides of the Atlantic Ocean. Continuing this proud tradition does not mean the shunning of other potential partners. On the contrary, presenting a strong united front could very well help bringing hesitant parties to the table once they feel secure that there are challengers to China's expansion in the cyber domain. Additionally, increasing

the joint cooperation within the transatlantic sphere – NATO for military affairs and offices for free trade for commercial affairs, for example – would bring a more holistic approach to the table and reduce the risk that the EU cyber strategy becomes inward-looking and reactive rather than adaptive and proactive.

3. The European Union should develop a joint strategy to fully address the risks of foreign state ownership in the internal market and prepare safeguards against serious intrusions into European infrastructure, both in terms of cyberspace and in terms of physical equipment relating to cyber functionality. The U.S. has made the protection of intellectual property a key issue in their interactions with Beijing, and the EU should be equally adamant on this point. EU protections in the internal market, the unique cross-border health care schemes that is afforded EU citizens for example, is unique in its kind and has aided in the Union revolutionising the concept of free movement of goods, services, and people within its borders. Arguably, such unique protections afforded to EU citizens should ideally apply even when the threat to our well-being originates from outside the EU's borders. Having the rights to what you earn, design, and create is fundamental for EU citizens and should – in the spirit of the Union's liberal agenda at large – be enforced no matter the origin of the threat. To this end, the EU should stand firm against Chinese expansionism and Beijing's intrusion into the lives and livelihoods of its citizens. In lieu of such union-wide agreements, there is always the possibility that single member states will attempt to reach individual bilateral agreements with China, risking the integrity of the united EU approach.

Thesaurus

RMA (Revolution in Military Affairs) – *hypothesis in military theory about the future of warfare, often connected to technological and organizational recommendations for military reform.*

Bibliography

Xinbo, W., (2000). U.S. Security Policy in Asia: Implications for China – U.S. Relations. *Contemporary Southeast Asia*. 22(3), pp. 479-497.

Richards, J., (2014). *Cyber-War: The Anatomy of The Global Security Threat*. London: Palgrave MacMillan.

Liang, Q. and Xiangsui, W., (1999). *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House Arts.

Segal, A., (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Aegis Paper Series* (1703), pp. 1-24.

Harold, S. W., Libicki, M. C., and Cevallos, A. S., (2016). *Getting to Yes with China in Cyberspace*. Santa Monica: RAND Corporation.

Clausewitz, C. V., Howard, M., Paret, P., Brodie, B., (1984). *On War.* 18th edn. Princeton, N.J.: Princeton University Press.

Bowler, T., (2020). *Huawei: Why is it being banned from the UK's 5G network?* [online]. BBC News. Available from: https://www.bbc.com/news/newsbeat-47041341.

Van der Meer, S., and Van der Putten, F. P., (2015). *US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations* [online]. The Hague: Clingendael Institute. [Viewed on November 20th, 2020]. Available from: www.jstor.org/stable/resrep05348.

European Commission and HR/VP., (2019). *Joint Communication to the European Parliament, the European Council and the Council: EU-China – a strategic outlook*. Strasbourg: the European Council. [Viewed on November 20th, 2020]. Available from: https://www.google.com

Richardson, S., (2020). China's Influence on the Global Human Rights System. *Brookings Institution*. [Viewed on December 12th, 2020]. Available from: https://www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_human_rights_richardson.pdf.

Xinbo, W., (2020). Sino-U.S. Strategic Competition and Asia-Pacific Security. In: A. Huiskinen, *Regional Security Outlook*. Canberra: CSCAP, pp. 13-16.

The World Bank., (2020). Current GDP of China in USD [online]. *The World Bank*. *Available from: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN*

Institute for Security & Development Policy., (2018). *Made in China 2025* [online] Stockholm: Instiute for Security & Development Policy. Available from: https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf

The Council on Foreign Relations., (2019). *Is "Made in China" a Threat to Global Trade?* [online]. The Council on Foreign Relations. Available from: https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

Capaccio, A., (2018). *U.S. Faces "Unprecedented Threat" From China on Tech Takeover* [online]. Bloomberg News. Available from: https://www.bloomberg.com/news/articles/2018-06-22/china-s-thousand-talents-called-key-in-seizing-u-s-expertise.

The National Bureau of Asian Research., (2017). *Update to the IP Commission Report – The Theft of American Intellectual Property: Reassessment of the Challenge and United States Policy* [online] Seattle: The National Bureau of Asian Research. Available from https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

Lee-Makiyama, H., (2018). *Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?* [online]. Brussels: ECIPE. Available from https://ecipe.org/wp-content/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf.

Council on Foreign Relations., (2020). *Cyber Operations Tracker* [online]. Council on Foreign Relations. Available from: https://www.cfr.org/cyber-operations.

Pepitone, J., (2015). *Obama: U.S. and China Reach Cyber-Espionage "Common Understanding"* [online]. NBC News. Available from: https://www.nbcnews.com/tech/security/obama-u-s-china-reach-cyber-spying-understanding-n433751.

Pramuk, J., (2020). *Trump Signs "Phase One" Trade Deal with China in Push to Stope Economic Conflict* [online]. CNBC, Available from: https://www.nbcnews.com/tech/security/obama-u-s-china-reach-cyber-spying-understanding-n433751.

European Commission Staff Working Document., (2020). *Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries* [online]. Brussels: The European Commission. Available from: https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158561.pdf.

Ludvig Hambraeus *is a Swedish-born law graduate and foreign policy professional. After having attained his first degree in law at Lund University he relocated to London, England, where he has pursued work with stakeholders in both the public and private sector on three continents in the fields of conflict avoidance and dispute settlement.*

U.S. PRIVATE EQUITY extraordinaire Stephen Schwartzman outlined it well: "In the 21st Century, China is no longer an elective, it is core curriculum". In order for stakeholders and policymakers to be successful in working with issues resulting from a rising China, an understanding of and appreciation for how China views the world and itself in it is key.

The American Response to Chinese Expansionism in Cyberspace – U.S. Policy Deconstructed for a European Audience is a short introduction to Chinese cyber expansionism and the U.S. response targeted towards those who wishes to attain fundamental insight in the field without any prior knowledge.

It was edited by Ludvig Hambraeus and authored by Ludvig Hambraeus and Katarina Tracz in an attempt to aid European decisionmakers and stakeholders in gaining greater understanding of one of the formulaic issues of the 21st century.

THE EUROPEAN LIBERAL FORUM (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 46 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard.

ISBN 978-2-39067-000-1