China and the World
The Yale Journal of International Affairs (YJIA) is a graduate student-run journal that aims to publish the best student and practitioner writing on international affairs. YJIA engages with the richness of its subject matter by elevating distinct perspectives and diverse areas of expertise among its writers and its editorship. YJIA seeks to embody the values and vision of the Jackson Institute for Global Affairs with which it is affiliated, chiefly by presenting innovative arguments and policy recommendations for global events and trends.

The Yale Journal of International Affairs would like to thank the Jackson Institute for Global Affairs for its generous support.

Visit our website at www.yalejournal.org. Our online platform contains both print and web-exclusive content.

Copyright © 2020 Yale Journal of International Affairs. All rights reserved. No part of this publication may be reproduced or transmitted in any form without the express written consent of the Yale Journal of International Affairs.
Evaluating Russia’s Pivot to Asia
By Ryan Nabil

Ryan Nabil, Yale Jackson graduate student, evaluates the extent to which Russia’s pivot to Asia has been successful, and what it means for American policymakers.

The “Value” of Propaganda
Predicting Political Crackdown in China Based on Text Data
By Julian Tszkin Chan and Weifeng Zhong

Economic policy experts Julian TszKin Chan and Weifeng Zhong develop a new policy index to predict the probability of future political crackdowns in China based on textual analysis of The People’s Daily, the official newspaper of the Chinese Communist Party.

Book Review: The Shanghai Free Taxi and Long Peace Street
By Rana Mitter

Rana Mitter, the Director of the Oxford China Centre, reviews Frank Langfitt’s The Shanghai Free Taxi: Journeys with the Hustlers and Rebels of the New China and Jonathan Chatwin’s Long Peace Street: A walk in modern China.
50  **Op-Ed: Why Peace Corps Should Stay in China**
By Krista Mangiardi

Krista Mangiardi, Yale Jackson graduate student and former Peace Corps volunteer, argues that the United States should not disband the Peace Corps program in China.

57  **Investment Screening for Developing Asia**
By Aaron Baum

Georgetown student Aaron Baum recommends that ASEAN member states create new investment screening mechanisms for foreign investment.

79  **Op-Ed: Countering China’s Maritime Threat Will Require a Larger U.S. Submarine Force**
By Pat Wiedorn

Pat Wiedorn, Yale Jackson graduate student and former U.S. Navy submarine officer, explains why the United States must invest in its submarine force to counter China’s maritime threat.
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>84</td>
<td>Photo Essay: Outsourced Lives in South Korea</td>
<td>By Tae Eom</td>
<td>In this thought-provoking photo essay, Tae Yeon portrays a nascent South Korean labor movement calling attention to the precarious lives of “irregular workers” in Seoul.</td>
</tr>
<tr>
<td>98</td>
<td>Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance</td>
<td>By Charles Smythe</td>
<td>Charles Smythe of the Georgetown School of Foreign Service argues that offensive strategies do not have an advantage over defensive strategies in cyberspace.</td>
</tr>
<tr>
<td>115</td>
<td>Interview with Staffan de Mistura</td>
<td>By Matt Trevithick</td>
<td>Yale Jackson graduate student and author Matthew Trevithick interviews Staffan de Mistura, the former UN Special Envoy for Syria, about successes and failures of the United Nations in Syria.</td>
</tr>
<tr>
<td>125</td>
<td>Op-Ed: Bit by Byte: Rebooting America’s Colombia Policy</td>
<td>By Eliot Pence</td>
<td>Defense and technology policy expert Eliot Pence argues that the United States should help the Colombian government acquire and develop new technologies to solve critical policy challenges.</td>
</tr>
<tr>
<td>131</td>
<td>A Social (Media) Contract: Reconciling American Freedom and Security in an Age of Online Radicalization and Extremism</td>
<td>By Tony Formica</td>
<td>Tony Formica, Yale Jackson graduate student and U.S. Army Downing Scholar, offers policy recommendations to counter the threat that online extremism and radicalization pose to American national security.</td>
</tr>
</tbody>
</table>
This edition, “China and the World,” represents the first regionally-themed issue in the Yale Journal of International Affairs’ 15-year history. The focus of this journal was motivated by our staff’s desire to highlight new and unique perspectives on China’s role in the global order. Since China’s rapprochement with the United States and its initiation of market-based reforms, the country has been on an upward trajectory of economic and diplomatic influence. However, as Chinese leaders become more assertive about China’s strategic interests and its state-led capitalism model, significant tensions have arisen with countries worldwide. These phenomena alone are more than worthy of academic discussion and analysis, but the past few months have added an additional dramatic factor to the balance of China’s role in the world: the spread of COVID-19.

As the global community navigates this unprecedented challenge, it is more important than ever for us to understand the implications of China’s domestic and foreign policies. I want to thank the authors and our staff for working together to produce pieces that shed light on China’s unique context in this moment in history. By bringing together cutting-edge work on Chinese foreign relations, security, and economic policy from leading graduate students, academics, and policymakers, it is our hope that the articles and op-eds in this issue provide valuable insights to the global community as we navigate this rapidly changing world.

Veronica Baker
Editor-in-Chief, 2019-2020
Yale Journal of International Affairs
INTRODUCTION

One of the virtues of good theory in international relations is to be able to assist policymakers in anticipating future developments.\(^1\) This is ever more important in the era of great power competition between the United States, China, Russia, and other powerful states. But what makes it particularly relevant also creates a distinct challenge: great power competition on a geopolitical scale is rare, and making good predictions of rare events is difficult.

Take China as an example: it is the only socialist country in history that, while remaining authoritarian, has abandoned central planning and grown its economy to one of the world’s largest. As a result of this uniqueness, there are not enough comparable precedents to draw statistical inferences about China’s major policy moves.\(^2\) Will President Xi Jinping’s administration enact more or less pro-market reforms? Will China concede to U.S. demands in their ongoing trade fight? Will the 2019 Hong Kong protests, which are ongoing at the time of this writing and have, at times, turned violent, face a Tiananmen-like crackdown by the Chinese government? The conventional toolkits used by political scientists are not adequate for answering specific, near-term questions of this nature.\(^3\) Additionally the domestic and international politics of these events are intertwined, further complicating the challenges of predicting future developments.

In this article, we employ a new approach hinging on machine learning to tackle these prediction problems. We start from an assumption that propaganda is an effective tool for moving public opinion and is therefore of indis-
pensable policy value to authoritarian regimes. Changes in propaganda content, therefore, often precede changes in actual policies. While fundamental socio-economic factors that drive policy changes may be too complex to sort out, natural language processing techniques can help us detect early warning signs in propaganda before policy changes take place.

In the context of China, we have conducted two studies that attempt to predict the Chinese government’s next moves by analyzing its official newspaper, *The People’s Daily*. The only input in these studies is the full text of the newspaper from when it was established in 1946 to the present day.

In the first study, we attempt to predict, on a quarterly basis, changes in China’s policy priorities by detecting changes in *The People’s Daily*’s editorial emphasis. The predictive algorithm has important implications for the U.S.-China trade negotiations. The second study tries to predict, on a daily basis, if and when the Chinese government will crack down on Hong Kong protesters. The assessment is made by comparing how closely *The People’s Daily*’s narrative regarding the ongoing Hong Kong protests resembles that regarding the Tiananmen protests.

While our studies have focused on China thus far, the machine learning framework is by no means only applicable to this context. We end this article with a discussion on how this method can be applied to a variety of other situations around the globe.

**THE “VALUE” OF PROPAGANDA**

Government propaganda in authoritarian regimes is commonly criticized, rightfully, for containing biases and disinformation and failing to meet modern standards of journalistic integrity. For this reason, researchers often avoid utilizing propaganda as a reliable source of information about a country of interest. However, it would be misguided to dismiss the value of propaganda in gleaning information about an authoritarian regime. In fact, propaganda content is exceptionally informative—not of the factual world, but of the authoritarian regime’s own views and intentions.

One example is the Soviet propaganda system. In the earlier years of the USSR, Vladimir Lenin asserted that “the whole task of the Communists is to
be able to convince the backward elements.” To fulfill that mission, he considered it a fundamental necessity “to transform the press from an organ which primarily reports the political news of the day into a serious organ for the economic education of the mass of the population.” Josef Stalin further elaborated that the purpose of such “economic education” is to “convince the masses by their own experience that [the party’s] policy is sound, thus ensuring the support of the working class and inducing the broad masses of the workers to follow [the party’s] lead.” In short, the regime relied on propaganda heavily to move public opinion ahead of policy so that subsequent economic policies could move forward with minimal resistance.

The Soviet propaganda model has been followed by China from its inception in 1949 through the modern era. As the literature on China’s propaganda system has shown, despite the transformation in the late 1970s from central planning to market economy, the Leninist model of indoctrination and mass mobilization remains quintessential in China’s political order. More recently, in 2016, President Xi Jinping made a high-profile visit to three major state news organizations and reiterated the role of China’s official media most explicitly: “all news media run by the party must work to speak for the party’s will and its propositions, and protect the party’s authority and unity.”

Because of a regime’s need to prepare the public for what is to come, a method that detects changes in propaganda content would be, effectively, a method that predicts changes in upcoming policies. This is the methodology underlying the series of Policy Change Index (PCI) projects, which we will describe in subsequent sections.

This approach is agnostic to the socio-economic factors that drive the changes in policies; those factors are traditionally at the center of social science research but are frequently too complex for generating specific predictions. Instead, we
attempt to detect early warning signals of those changes in the regime’s own words—words that are typically observed just before the changes take place.

One analogy in macroeconomics is the inverted yield curve. Many economists believe that the yield curve tends to invert when a recession is afoot, making it a near-term leading indicator. While the fundamental causes of a recession may be complex, detecting an inversion of the yield curve, as a near-term forecasting exercise, does not require understanding those fundamental causes. Similarly, in this approach to predicting policy changes, the exact socio-economic drivers of the changes are not essential to making the predictions.

POLICY CHANGE INDEX FOR CHINA

China scholars tend to focus their attention on the Chinese economy and the government’s prominent role in driving the national industrialization process. While there are voluminous data on the Chinese economy, until now there have been no quantitative indicators of the Chinese government’s policy priorities over a long period of time.

In the first study, we fill that gap by devising the first of such measures, the Policy Change Index for China (PCI-China hereafter), a predictive indicator of major policy moves from the first quarter of 1951 to the third quarter of 2019, and it will be updated on a quarterly basis in the future. This indicator not only helps us understand China’s industrialization process in the past but also allows us to make short-term predictions about its future.

As elaborated in the previous section, we approach the problem of predicting changes in policy priorities by detecting changes in The People’s Daily’s editorial emphasis. Since editorial emphasis is an abstract concept, we proxy for it using a front-page classifier that predicts
whether an article appears on the front page—the most prominent space in a newspaper—based on the text of articles in a certain period.14

Figure 1 outlines the method of constructing the PCI-China. For each five-year window, we build a front-page classifier to read the text of the articles published within that time and learn to tell front-page articles apart.15 Whatever patterns the algorithm learns in this step would constitute a fairly good understanding of the editorial emphasis during the five years in question. We then deploy the same front-page classifier to the quarter following the five-year window and examine how the performance is. If the editorial emphasis is more or less the same, the algorithm should perform just as well in the new quarter as it did in the previous five years. But if the performance is very different, it would mean the editorial emphasis has changed from the preceding five years to the next quarter. After all, the editorial emphasis is fundamentally a reflection of what the government-controlled editors consider worthy of front-page status, and, implicitly, which content is not so deserving.

We define the difference in performance between the two classification tasks—the one for the five-year period and the one for the following quarter—as the

---

**Figure 1. Outline of PCI-China algorithm**

- **Articles in previous 5 years**
- **Articles in next quarter**
- **Train a front-page classifier**
- **Deploy**
PCI-China (for that particular quarter). When the indicator’s value is close to zero, it means the two classification tasks are performing similarly, indicating a stable editorial emphasis. In contrast, if the indicator’s value is high, it suggests a shift in editorial emphasis.

Finally, to produce a time series, we move the training period quarter by quarter, generating a quarterly indicator from the first quarter of 1951 to the present.

Figure 2 shows the PCI-China together with the set of events that academic researchers generally consider important in the history of the Chinese economy in the modern era. For an indicator to be predictive in this context, it would have to have two properties: (1) in terms of timing, it should spike up before an actual policy change occurs; and (2) in terms of substance, since a spike represents different classification performance between the quarter in question and the previous five years, the content of the articles misclassified by the algorithm should be consistent with the nature of the actual policy change preceded by the spike. In other words, if the indicator spikes up before the government changes policy A to policy B, and if the misclassified articles around the spike correspond to a shift from topics related to policy A to that
related to policy B, then the indicator is considered predictive of that particular policy change. As the figure shows, the PCI-China typically precedes the labeled major events.\textsuperscript{17} Moreover, as we have demonstrated in our earlier writings, the substance of those spikes is consistent with the policy changes they precede.\textsuperscript{18}

A good example is the 2005 reform slow-down under former President Hu Jintao, largely attributed to his “Harmonious Society” initiative. This policy change is picked up by the indicator in 2004—five quarters ahead of time. Figure 3 provides a zoomed-in view around that time. At the time of the 2004 spike, the articles misclassified by the algorithm represent a shift away from prioritizing pro-market reforms, such as privatizing state-owned enterprises and allowing private companies wider and fairer access to various sectors in the economy, to an emphasis on tackling a set of social issues, such as income inequality, poverty, and regional imbalance in development, with interventionist government measures. These latter policies would be consistent with government interventions that undermine the role of the market in allocating resources, which is what did occur the next year with the “Harmonious Society” initiative.

\textbf{Figure 3: PCI-China and major policy events, 1997 Q1 to 2007 Q4}
The tool also has important implications for the ongoing U.S.-China trade fight. The indicator shows two recent upticks, in the first quarter of 2018 and, subsequently, the first quarter of 2019. In both cases, the editorial changes suggest that China is taking increasingly strident positions in domestic issues and foreign policy. The newspaper coverage emphasizes, even more than before, the importance of state-owned enterprises and using interventionist measures to boost the economy, and it argues for taking a leadership position on the global stage.

As we have written elsewhere, this editorial emphasis is inconsistent with U.S. demands in the trade negotiations, namely, that China reduce the role of government in its economy. Using the indicator, we have predicted consistently since the beginning of the year that China will not agree to making such changes as part of a trade deal with the United States. What has transpired so far has been in line with our prediction.

POLICY CHANGE INDEX FOR CRACKDOWN

The year 2019 saw a series of protests in Hong Kong that persisted to the time of this writing, stirring anti-China sentiment and spurring speculation of a Tiananmen-like crackdown by the Chinese government on the semi-autonomous city.

In the second study, we attempt to predict if and when such a crackdown will occur using a method similar to the PCI-China. The output, which we call the Policy Change Index for Crackdown (PCI-Crackdown hereafter), gives a daily estimate of how close in time the 2019 Hong Kong protests are to the Tiananmen crackdown in 1989. The closer the PCI-Crackdown’s output is to June 4, 1989, the more likely a similar crackdown will happen in Hong Kong as well.

Two challenges stand out in predicting the occurrence of such a crackdown: (1) the protests and the government’s responses to them are highly interactive, and (2) a Tiananmen-like crackdown is a particularly rare event; it only happened once before in China.

To overcome these challenges, we rely on the same hypothesis as before — propaganda precedes actions. The idea is, even though authoritarian regimes do
not have free and fair elections, public opinion still matters to the government, especially regarding such contentious, destructive policies as a crackdown. In the days leading up to the June 4, 1989 crackdown on Tiananmen protesters, *The People’s Daily* drastically changed its rhetoric on the protests. “Demonstrators” and “protesters” became “rioters,” and the students, who used to “have a good heart,” now only wanted to “destroy the country’s future.” As described earlier, we believe that the Chinese government’s playbook in this regard has not changed since 1989, and that the same approach applies to the case of Hong Kong: if the Chinese government were to crack down on the protests, it would also change its narrative of the protesters in order to prime public opinion to support government action. Our machine learning program is built to detect such a narrative change.

Figure 4 shows the method of constructing the PCI-Crackdown, which is similar to that shown in Figure 2. We first train a date classifier that predicts the date of publication for an article using the text of *People’s Daily* articles in 1989 that are related to the Tiananmen protests. We use the same learning-from-examples approach, except that, here, instead of the algorithm learning what kind of text appears in articles on the front page, it learns what kind of text appears in articles on each date leading up to the Tiananmen crackdown. After training the algorithm, we feed it the recent articles on the

---

**Figure 4: Outline of PCI-Crackdown algorithm**

Articles leading up to Tiananmen crackdown

- - -

Train a date classifier

Recent articles on HK protests

Calculate the “as-if” date
Hong Kong protests and ask it to determine the predicted dates for the new articles. Because the model was trained using articles from 1989, it will likely make “mistakes” when processing articles published in the present day, predicting that they are from 1989 as well. But this error is exactly what we aim for: each (factual) date in the Hong Kong protest timeline is cast back—by “mistake”—to the Tiananmen timeline, and the counterfactual date assigned to that (factual) date is defined as the PCI-Crackdown for the Hong Kong protests on that day.

Figure 5 shows the PCI-Crackdown for the 2019 Hong Kong protests as well as a set of events related to the protests that indicate the change in tension. The horizontal axis shows the current timeline of the Hong Kong protests, and the vertical axis shows the PCI-Crackdown, the counterfactual timeline leading up to the Tiananmen crackdown. Each data point in this time series gives an “as-if” date in the Tiananmen timeline to the (factual) date in the Hong Kong timeline, serving as a barometer of tension. As the PCI-Crackdown ascends toward the dashed line on June 4, 1989, the likelihood of a Tiananmen-like crackdown in Hong Kong increases.
When interpreting the output of the PCI-Crackdown model, it is important to keep in mind that the tension generated by protests does not always increase in a linear fashion. While the level of tension in the month or so leading up to the Tiananmen crackdown was largely increasing throughout, the evolution of tension in the ongoing Hong Kong protests can and did have its ups and downs, which is what Figure 5 captures. For example, the spike of the PCI-Crackdown on August 5, 2019, when the Chinese authorities were conducting the first anti-riot drill near the Hong Kong border, reached the level of rhetoric seen on May 26, 1989—less than ten days before the Tiananmen crackdown. The tension somewhat eased off in September and October, which was picked up by the indicator as it showed less frequent movements and registered lower values. However, the relative calmness proved to be short-lived; the more recent violent confrontation between protesters and the police in November brought the indicator back to a higher level.

The Chinese government’s narrative regarding Hong Kong is also very responsive to the dynamics of U.S.-China relations. For example, on October 14, 2019, after the U.S. and China agreed to signing a “phase-one” trade deal, the indicator dropped from the previous high of May 19, 1989 to May 8, 1989, almost a month away from the June 4, 1989 crackdown. However, just three days later, it bounced back to May 16, 1989 after the U.S. House of Representatives passed the Hong Kong Human Rights and Democracy Act, a bill the Chinese government claimed interfered in its internal affairs.

Since both the Hong Kong protests and the U.S.-China trade negotiations are still ongoing, the PCI-Crackdown remains a useful way to gauge how the events will unfold.

**POTENTIAL APPLICATIONS**

*The People’s Daily* is by no means a unique case in which authoritarian propaganda has predictive value. The same method can be readily replicated on other authoritarian regimes with state-controlled media. *The People’s Daily* is to China as the Rodong Sinmun is to North Korea, the Granma is to Cuba, and the Nhân Dân is to Vietnam. Extending the PCI project series in this direction is part of our ongoing efforts.
In addition, the PCI algorithms are also applicable to domestic politics. Any politician or otherwise publicly accountable decision-maker may, for various reasons, find it necessary to alter their words before changing their actions. Imagine a liberal-leaning legislator who decides to support a conservative-leaning bill. Due to political pressure—be it from their legislative allies or their constituents—it may be crucial that the legislator justifies their unusual vote in advance. The PCI framework can enable us to predict changes in their actions based on changes in their words.

We leave it to future research to explore these different contexts in which our methodology can be applied.

ABOUT THE AUTHORS

Julian TszKin Chan is a Managing Economist and Lead Data Scientist at Bates White Economic Consulting.

Weifeng Zhong is a Senior Research Fellow at the Mercatus Center at George Mason University.

Chan and Zhong are core maintainers of the Policy Change Index, a series of open-source machine learning projects. More about this line of their work can be found at: policychangeindex.org.

ENDNOTES


2. While some of the mentioned characteristics apply to a few other countries, the uniqueness of this combination makes it difficult to find reference points.

3. Paul Collier, for example, notes that his model cannot be used to predict civil war. “[It] can tell you the sort of countries that are most at risk. But it cannot tell you whether Sierra Leone will have another civil war next year.” Paul
Collier, The Bottom Billion: Why the Poorest Countries Are Failing and What Can Be Done About It (Oxford: Oxford University Press, 2008). One can see this drawback more generally, in the literature on the causes and correlates of war. The typical approach taken by most models starts with a cross-country approach and focuses on identifying the conditions that are most conducive to war. But the indicators are blunt in that they are typically measured by year, not by day or month, and they are not meant to be interpreted as predictions on any specific country in the sample. See, e.g., Nathaniel Beck, Gary King, and Langche Zeng, “Improving Quantitative Studies of International Conflict: A Conjecture,” American Political Science Review 94, no. 1 (March 2000); Scott de Marchi, Christopher Gelpi, and Jeffrey Grynaviski, “Untangling Neural Nets,” American Political Science Review 98, no. 2 (May 2004); Nathaniel Beck, Gary King, and Langche Zeng, “Theory and Evidence in International Conflict: A Response to de Marchi, Gelpi, and Grynaviski,” American Political Science Review 98, no. 2 (May 2004); Kristian Skrede Gleditsch and Michael Ward, “Forecasting Is Difficult, Especially About the Future: Using Contentious Issues to Forecast Interstate Disputes,” Journal of Peace Research 50, no. 1 (January 2013).

4. Communications scholars have long argued that propaganda “works.” See, e.g., Walter Lippmann, Public Opinion (New York: MacMillan Co., 1922) and Harold Lasswell, Propaganda Technique in the World War (Oxford: Knopf, 1927). In recent years, empirical studies have shown that media can indeed have a significant effect on political outcomes, especially in authoritarian or totalitarian regimes. A few examples in this literature are: Matthew Gentzkow and Jesse Shapiro, “Media, Education and Anti-Americanism in the Muslim World,” Journal of Economic Perspectives 18, no. 3 (Summer 2004); David Yanagizawa-Drott, “Propaganda and Conflict: Evidence from the Rwandan Genocide,” The Quarterly Journal of Economics 129, no. 4 (November 2014); Maja Adena, Ruben Enikolopov, Maria Petrova, Veronica Santarosa, and Ekaterina Zhuravskaya, “Radio and the Rise of the Nazis in Prewar Germany,” The Quarterly Journal of Economics 130, no. 4 (November 2015).


6. Ibid., 162.

7. Ibid., 18.


10. One may wonder if the Chinese government uses propaganda outlets to test messages—that is, experimenting with different policy messages to determine their effect on the public. Such experimentation has been observed in other circumstances, such as Russia reportedly testing new disinformation tactics in a Facebook campaign in parts of Africa. See Davey Alba and Sheera Frenkel, “Russia Tests New Disinformation Tactics in Africa to Expand Influence,” The New York Times, October 30, 2019. We are not aware of such message experimentation in The People’s Daily, likely because it is too prominent for running experiments. Testing in Chinese local newspapers, however, is certainly plausible.


12. The policy indicator closest to what we focus on is the economic policy uncertainty index pioneered by Scott Baker, Nicholas Bloom and Steven Davis, “Measuring Economic Policy Uncertainty,” The Quarterly Journal of Economics 131, no. 4 (November 2016). An implementation of their framework in the context of China is done by Yun Huang and Paul Luk, “Measuring Economic Policy Uncertainty in China,” working paper (2018). However, there is a clear distinction between policy priorities and policy uncertainty; the realization of uncertainty may imply a change (in priorities), but priorities, if well-defined and strictly held, contain little uncertainty.

13. The most up-to-date PCI-China is available at: policychangeindex.org.

14. In the machine learning literature, this approach is called supervised learning, where the algorithm is trained under the “supervision” of known examples provided by researchers (e.g., front-page versus non-front-page articles) and is designed to learn the patterns that set them apart.


17. Here, we use the words “typically precedes” because, in neural network models, a formal statistical inference procedure remains an open question in the literature. We leave that issue to future research.


21. The Tiananmen protests started on April 15, 1989, after the death of Hu Yaobang, a pro-reform Chinese leader. The protesters sought democracy, freedom of speech, and greater accountability of the government, among other things. It ended on June 4, 1989, when the government sent troops to Tiananmen Square to suppress the protests.

22. The indicator is plotted up to December 8, 2019. For future daily updates, see: policychangeindex.org.
Since the Soviet Union’s dissolution in December 1991, the Russian government has pursued two interrelated goals: to create a stronger economy and reestablish Russia as a great power. In pursuit of these goals, Moscow initially sought close relations with the West in the early 1990s. However, the Russian foreign policy elite became disappointed by the West’s refusal to accept Russia as an equal power and NATO’s expansion in 1999 and 2004. With Russia’s deteriorating relations with the West and Asia’s growing economic impor-
tance, the Kremlin gradually pursued a multi-vectored foreign policy, in which China and other Asian countries played an important part. Russia and China found several venues for cooperation, including strengthening bilateral trade and investment, opposing the U.S.-led global order through multilateral institutions, and ensuring stability in the post-Soviet space. Western sanctions following Russia's annexation of Crimea in 2014 accelerated Russia-China relations as Russian leaders sought to reduce Russia's economic dependence on the West. At the same time, Moscow sought to avoid becoming China's junior partner by restraining China through multilateral organizations and strengthening ties with other Asian countries, like Vietnam and South Korea. In the long term, as the gap between Russian and Chinese economic and military capabilities widens, the basis of Russia-China relations—trade, security cooperation, and stability in the post-Soviet space—are likely to weaken. Moscow's management of the changing Russia-China relations will shape Russia's future relations with China and the West.

INTRODUCTION

Since the Soviet Union's dissolution in December 1991, the Russian government has pursued two interrelated goals: to create a stronger economy and to restore Russia's status as a great power. In pursuit of those goals, the Russian government initially sought to improve relations with the West and establish Russia as a Western power equal to Europe and the United States. By the early 2000s, as a result of Western military campaigns in the former Yugoslavia and the North Atlantic Treaty Organization's (NATO) expansion, it became clear to Russian leaders that the West would not accept Russia “as an equal partner.” After the 2008 financial crisis, which affected Europe and the United States disproportionately more than Asian economies, China emerged as the world’s second-largest economy, and Chinese diplomacy became more assertive under Hu Jintao. Hu argued that China should take “an active role in international affairs and work to make the international order more just and equitable.” Under this changing international environment—with a West largely ignoring Russian security interests and Beijing playing an increasingly assertive role—the Kremlin decided to pursue a multi-vectored foreign policy, in which Sino-Russian relations would feature more prominently. After the 2014 Crimean crisis, Moscow’s relations with the West deteriorated further, which gave an additional incentive for the Kremlin to strengthen Russia-China relations. At the same time, to avoid becoming a junior partner to China,
Russia sought to contain China through multilateral organizations, like the Eurasian Economic Union (EAEU) and Shanghai Cooperation Organization (SCO), and pursue closer relations with other Asian countries.\(^6\)

Despite the Kremlin’s increasing emphasis on China and other Asian countries, the results of Russia’s pivot to China and Asia are mixed. Except for trade with China and arms sales in India and Vietnam, Russia’s footprint in Asia remains modest.\(^7\) In the short term, Russia’s ties with China helped the Kremlin achieve a limited degree of tactical success. As Europe and the United States restricted Russia’s access to the Western markets, exports to China and the access to Chinese capital markets helped Russia partially cope with the economic effects of the sanctions. However, Russia-China relations have not been able to offset the fall in Russia’s overall trade and investment levels due to the sanctions.\(^8\) It is also unclear that Russia-China cooperation in multilateral forums helped Russia achieve its strategic objectives, like preventing NATO-led military actions in the Balkans during the late 1990s and NATO’s expansion in 1999 and 2003.\(^9\)

In the long term, Russia-China relations face several challenges that Russian leaders will need to manage. As the economic performance of China and Russia diverge and Beijing’s commercial advantage relative to Moscow grows, Russia risks becoming a junior partner to China and losing its strategic autonomy.\(^10\) Beijing is also gradually eroding Moscow’s influence in the former Soviet space, notably Central Asia, where China is the now largest trade partner for all of the five Central Asian countries.\(^11\) In the context of arms sales, which underpinned bilateral relations since the 1990s, China is rapidly modernizing its military-industrial complex and increasingly competing with Russia in the international arms market.\(^12\) Given the changing roles of Russia and China, the Kremlin faces two critical questions: how does Moscow manage its relations with Beijing in pursuit of Russia’s strategic objectives?\(^13\) What are the long-term challenges to Russia-China relations, and what do such challenges mean for Russia’s relations with the West?\(^14\) The Kremlin’s response to these two questions will shape Russia’s relations with China and the West in the coming years.

**INITIAL RAPPROCHEMENT WITH THE WEST**

After the USSR’s dissolution, the Kremlin initially sought close relations with the United States and the European Union in pursuit of Russia’s strategic ob-
jectives.\textsuperscript{15} Moscow wanted the West to accept Russia as an equal or at least an essential partner of the “global North” and perceived positive relations with the United States and Europe as the best way to achieve that goal.\textsuperscript{16} Russian leaders thought that by rejecting communism, adopting democratic principles, and transitioning to a market economy, Russia would immediately be accepted as a member of the Western economic and security structures.\textsuperscript{17} As Alexander Lukin describes, this strategy underpinned the Kremlin’s broader goal of making Russia part of a “united Europe stretching from Lisbon to Vladivostok” and creating a Euro-Atlantic alliance.\textsuperscript{18} Therefore, Russia sought a role that would allow the Kremlin to shape international policies, especially in security affairs, jointly with Europe and the United States.\textsuperscript{19}

However, Russia’s perception that the West would immediately welcome Russia as a member of the Euro-Atlantic community turned out to be a mistake.\textsuperscript{20} From the Russian point of view, despite a series of efforts to improve relations with the West, Russia was unfairly treated each time.\textsuperscript{21} During the 1990s, despite Russia’s attempt to build a security partnership with the West, NATO admitted Poland, Hungary, and the Czech Republic as member states in 1999 and undertook a 78-day military campaign in Yugoslavia without Russian approval and UN Security Council authorization.\textsuperscript{22} Furthermore, in spite of Moscow’s support during the Afghanistan War, President George W. Bush announced that the United States would withdraw from the Anti-Ballistic Missile Treaty in 2002 and that NATO would admit Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, and Slovenia as members in 2004—which the Kremlin perceived as yet another Western betrayal.\textsuperscript{23} Russian leaders viewed NATO’s enlargement and its military operations as a betrayal because it effectively excluded Russia from the Western security architecture and its decision-making processes.\textsuperscript{24}

By 2007, it became clear to the Kremlin that the West would not accept Russia as a partner within NATO or other Western-led security architecture.\textsuperscript{25}
This understanding gradually led the Kremlin to advocate a multipolar world, in which Russia would seek to play an important role. During his February 2007 Munich Security Conference speech, Vladimir Putin highlighted the growing economic and political importance of non-Western countries, like China and India, whose combined GDP already surpassed that of the United States. While Russia’s disillusion with the West predated Putin’s 2007 Munich speech, this speech marked an official point after which non-Western countries, especially China, would play a more important role in Russia’s multi-vectored foreign policy.

**STRATEGIC INCENTIVES FOR RELATIONS WITH CHINA**

Given China’s growing role as an economic and political player, closer relations with China is critical to Russia’s strategic objectives for at least three reasons. First, the Kremlin recognizes that while it wants to challenge U.S. hegemony, Russia cannot do so alone. By cooperating with China, Russia can create the perception of a united non-Western front and gain strategic leverage in dealing with the West. For instance, by cooperating with China in international organizations like SCO, Russia has sought to create alternative multilateral institutions that could provide a counterweight to Western organizations like NATO and Bretton Woods institutions. Therefore, Chinese support is essential for effective opposition against what Moscow perceives to be U.S.-led hegemony.

Second, stronger ties with China allow Russia to diversify its trade and investment relations and reduce its economic dependence on Europe and the United States. As the world’s second-largest economy, China offers Russia significant trade and investment opportunities, which has become all the more critical since the Ukraine crisis. In this context, closer economic ties with China are especially crucial for the economic development of the Russian Far East. Although the Far Eastern federal district comprises 36.4 percent of Russia’s total area, it contributed only 5.5 percent...
to the country’s GDP growth in 2015. Given this economic backwardness, Vladimir Putin declared the Far East’s economic development as a national priority, calling it “the most important geopolitical task facing the Russian Federation” today. As the largest economy in northeastern Asia, China can help promote growth in the region by increasing trade and infrastructure investment.

### TRENDS IN CHINESE INVESTMENT IN RUSSIA

After the 2008 financial crisis, Russian leaders sought to improve its economy by attracting foreign investment and bolstered its efforts to attract Chinese investment. In the aftermath of the financial crisis, global energy prices experienced a sharp decline, heavily affecting the Russian economy. Following the crisis, Russian leaders prioritized foreign economic relations, leading to economic considerations gaining “an unprecedented centrality” in Russian strategic thinking. As China emerged relatively unscathed from the crisis, it catalyzed Sino-Russian relations—as the Kremlin sought closer trade and investment ties with China in a bid to diversify Russia’s international trade and investment relations, especially in the energy and banking sectors. As a result, Russian leaders became more willing to put aside previous tensions in Sino-Russian relations in pursuit of increased investment from China. Due to increased Sino-Russian economic cooperation, Chinese investment in Russia continued to grow well after 2009. In 2009, Russia attracted only $780 million in Chinese investment, or approximately 1.39 percent of China’s total investment worldwide, making Russia the fourteenth largest recipient of Chinese investment (Figure 1). Following the Kremlin’s efforts, Chinese investment in Russia increased steadily, reaching a peak of $6.25 billion in 2013 (Figure 1). As a result, Russia ranked as the fourth-largest recipient of Chinese investment in 2013 (after the United States, Australia, and Britain), accounting for 7.73 percent of total Chinese investment that year (Table A1). The 2014 Ukraine conflict created new opportunities for strengthening economic relations between China and Russia. After Russia annexed Crimea following a controversial referendum and Russian-armed rebels shot down a Malaysian Airlines flight, the United States and the European Union imposed sanctions against Russia. Such sanctions severely limited Russian energy companies and financial institutions’ access to American and European capital markets. Already suffering under low energy prices, the Russian econ-
omy sank even further due to the sanctions, with Russia’s GDP declining by 3.8 percent in 2015 and 0.6 percent in 2016. Under these circumstances, Vladimir Putin bolstered his diplomatic outreach to China for “an economic lifeline,” with an objective to secure deals for the Russian energy sector and financing for Russian banks and energy companies. Consequently, in October 2014 alone, Chinese companies and financial institutions signed forty deals with Russian entities in sectors ranging from energy to technology. These deals included an agreement in which “Chinese banks agreed to provide credit lines worth more than $4.5 billion to Russian banks and companies,” according to the Wall Street Journal. Additionally, the Russian government managed to secure several other high-profile deals, including a 2019 agreement to construct “a $55 billion pipeline” to deliver gas from Siberia to northeast China.

Despite Russia’s best efforts, China did not turn out to be the economic lifeline that Moscow had expected. Due to the extraterritorial application of U.S. sanctions, Chinese companies face the risk of incurring U.S. civil penalties.

Figure 1. Chinese investment in Russia and the world, 2009-2018

Source: Author using data provided by the American Enterprise Institute and Heritage Foundation (2019)
and criminal prosecution by doing business with sanctioned Russian entities.\(^53\) Such considerations likely played a major role in reducing Chinese investment in Russia.\(^54\) Between 2013 and 2018, Chinese investment in Russia from $6.25 billion to $480 million, representing a 92.3 percent decline (Figure 1). In contrast, Chinese investment worldwide grew by 121.3 percent during the same period (Figure 1). Therefore, economic evidence suggests that, rather than filling the void created by Western sanctions, Chinese investment in Russia decreased dramatically after the Ukraine crisis. As a result, despite expectations that Russia’s pivot to Asia brought Moscow and Beijing closer together, Sino-Russian investment relations suffered greatly due to Russia’s annexation of Crimea.

**TRENDS IN RUSSIA-CHINA TRADE RELATIONS**

In addition to courting Chinese investment, the Russian government also took steps to expand trade relations with China. Following the 2008 financial crisis, which affected the Western economies disproportionately more than the

**Figure 2. Russia-China bilateral trade (in goods), 2007-2018**

![Graph showing Russia-China bilateral trade](image)

Source: Author using data from the UN International Trade Statistics Database (2020)\(^57\)
Chinese economy, Russian leaders expanded their diplomatic outreach to China. In the aftermath of this outreach, Russian exports to China rose by 77.3 percent between 2008 and 2014, while Russian imports from China increased by 46.3 percent (Figure 2). However, Russia’s exports to China decreased by 24.3 percent between 2014 and 2015 due to falling oil prices and the struggling Russian economy (Figure 2). After Moscow sought to improve its economic relations with China following the Ukraine conflict, Russian exports to China increased again, eventually reaching $56 billion in 2019 (Figure 2).

Despite this increase in bilateral trade volume, Russia-China economic relations remain skewed in Beijing’s favor. In particular, the size of the Chinese economy gives Beijing an upper hand in bilateral relations. In 1991, the Chinese economy was roughly the same size as the Russian economy. However, due to China’s superior economic performance, the Chinese economy is now at least six times larger than the Russian economy. This difference in the size of the economies means that Chinese markets are much more important for the Russian economy than Russian markets are for China. In 2018, Russia ranked as only the 12th largest export destination for China, accounting for only 1.9 percent of Chinese exports (Table 1). In contrast, China ranked as the most important market for Russian exports, accounting for 12.5 percent of Russian exports (Table 1). Even with a slowing Chinese economy, China’s current growth rate was 4.3 percentage points higher than that of Russia in

### Table 1. Largest export markets of Russia and China (in goods), 2018

<table>
<thead>
<tr>
<th>Russia’s Largest Export Markets</th>
<th>Share of Total Russian Exports</th>
<th>China’s Largest Export Markets</th>
<th>Share of Total Chinese Exports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. China</td>
<td>12.5%</td>
<td>1. United States</td>
<td>19.2%</td>
</tr>
<tr>
<td>2. Netherlands</td>
<td>9.7%</td>
<td>2. Hong Kong</td>
<td>12.1%</td>
</tr>
<tr>
<td>3. Germany</td>
<td>7.6%</td>
<td>3. Japan</td>
<td>5.9%</td>
</tr>
<tr>
<td>4. Belarus</td>
<td>4.9%</td>
<td>4. South Korea</td>
<td>4.4%</td>
</tr>
<tr>
<td>5. South Korea</td>
<td>4.8%</td>
<td>5. Vietnam</td>
<td>3.4%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12. Russia</td>
<td>1.9%</td>
</tr>
</tbody>
</table>

Source: Author’s using data from the UN International Trade Statistics Database (2020)
Due to the larger size and higher growth rate of the Chinese economy relative to the Russian economy, the gap between the Chinese and Russian economies is only likely to widen, which will further diminish Russia’s attractiveness as an economic partner for China.

The growing economic advantage of Beijing relative to Russia becomes even more evident upon examining the trends in China-Russia trade relations. Since 2007, Russia ran a trade deficit against China every year until 2018, when Russia registered a trade surplus of $3.8 billion due to rising oil prices (Figure 2). Furthermore, Russia’s exports to China remain heavily dependent on energy and raw materials, making Russia vulnerable to fluctuations in global oil and raw material prices. Petroleum and raw materials—crude and refined petroleum, coal, iron and lead ore, raw nickel, and wood materials—accounted for roughly three-fourths of Russia’s exports to China in 2017. In contrast, China’s exports to Russia are diversified and mostly include advanced manufactured products, which helps create more jobs in the process of producing such goods. For instance, electronics comprised roughly one-third of China’s exports, while textiles, chemical products, and vehicle parts accounted for one-fourth of China’s exports to Russia in 2017. In this context, China-Russia trade relations is characteristic of China’s trade relations with resource-rich African countries like Egypt, where energy and raw materials also account for roughly three-fourths of total exports to China. Consequently, Russia’s export receipts to China remain highly vulnerable to fluctuating oil prices and changing energy consumption trends in China.

RUSSIA-CHINA TRADE IN ARMS

Russian arms exports to China are a crucial aspect of bilateral relations; however, the trends in weapons sales do not bode well for Russia. After the Tiananmen Square incident, China found itself cut off from the Western arms markets during the 1990s and relied on Russian imports for equipping the People’s Liberation Army. As a result, Russia became the dominant military supplier to China by the 1990s, with Russian arms exports to China increasing from approximately $1 billion to $3.1 billion between 1992 and 2005 (Figure 3). However, since the mid-2000s, the Chinese government has undertaken substantial efforts to modernize its military-industrial complex. Between 2005 and 2018, the Chinese government more than tripled its military budget, and China is now “the world’s second-largest arms producer,
trailing the United States and ahead of Russia. This modernization has not only reduced the Chinese demand for Russian military imports, but Chinese arms suppliers are also competing with Russian military producers, especially in countries that cannot afford arms from the United States and European countries. As a result, Russian arms exports to China have diminished considerably, with exports decreasing to pre-2000 levels by 2015 (Figure 3).

The Chinese military-industrial complex’s recent transformation poses several challenges to Russia-China relations. Due to improvements in military capability, Chinese producers can now mostly replicate Soviet-era weapons and have started demanding more advanced Russian weapons, like anti-missile detection systems and sophisticated fighter jets. However, Russian security experts are increasingly concerned about China’s replication of Russian weapons through reverse-engineering and the theft of Russian designs. For instance, Russian analysts accused Chinese producers of copying the Russian-made Sukhoi Su-33 to manufacture Shenyang J-15 aircraft (although this strategy did not work out well for China as the J-15 planes began to experience frequent flight control system problems and crashed several times). Nevertheless, Bei-
jing continues to lobby Moscow for increasingly sophisticated military exports, including high-performance fighter jets and surface-to-air missile systems.74

Until 2014, the Russian government declined to sell its most sophisticated arms to China.75 However, faced with Western sanctions, economic difficulties, and stagnant arms sales, the Kremlin reasoned that Chinese producers would eventually be able to design advanced fighter jets and approved the sale of 24 Sukhoi Su-35 fighter jets, making China the first country to purchase this new generation of fighter jets.76 However, as the Chinese government further upgrades its military capability, Russian exporters might find it challenging to stay competitive in the Chinese defense market.77 As a result, Russian arms exporters are increasingly looking to China’s security rivals, notably India and Vietnam, for exports (see “Relations with Other Asian Countries”).78 Consequently, in the long term, the prospects for strong Sino-Russian relations based on Russian arms exports to China remain weak.79

RUSSIA-CHINA SECURITY COOPERATION

Beyond arms trade, Moscow and Beijing have also identified several areas for security cooperation. First, since the 1990s, the two countries have taken active steps to resolve border disputes, demilitarize the Russia-China border, and lift restrictions on Sino-Russian trade and immigration along the border regions.80 Second, despite occasional internal disagreements, the two countries support each other, or at least refrain from active opposition, on issues that the other side regards as “core interests.”81 For instance, the Russian government publicly supports the “One China” policy by not recognizing Taiwan and remains neutral on China’s military buildup in the South China Sea—two issues that the Chinese government considers as “core interests.”82 Conversely, Beijing does not contest Moscow’s geopolitical interests in Russia’s sphere of influence, like the Balkans and the Caucasus.83 For instance, Beijing refrained from applying Western sanctions against Russia and abstained from two United Nations resolutions on the Crimean independence referendum and its subsequent annexation by Russia.84

Notwithstanding this perception of closer security ties, it is unlikely that Russia and China will ultimately finalize any form of a collective security agreement. Compared to Russia, China benefits significantly more from the U.S.-led international order through trade and investment ties with the West.85
While the Chinese government is committed to ensuring its territorial integrity and maintaining core Chinese security interests in the East and South China Seas, Beijing seeks to avoid a military confrontation with the United States. Furthermore, Beijing finds Moscow’s military pursuits, like the 2008 Georgian War, untactful, and has been unwilling to take sides in the Russian conflicts in the Caucasus region. For instance, due to Chinese opposition, “SCO declined to publicly endorse Russia’s account of its August 2008 war with Georgia (Moscow claimed that the Georgian army attacked first, an assertion implicitly recognized even by the U.S. ambassador to Russia).” Furthermore, in the event of an international conflict involving China, Russia’s commitment and capability to assist China militarily remains unclear. As a result, despite Moscow’s lobbying, Beijing declined to convert the SCO into a full-blown security alliance that could serve as a counterweight to NATO.

Closer Russia-China security ties might not serve Russia’s interests in the long term either. China’s growing economic power, military budget, and rapidly modernizing military-industrial complex means that the country has a military advantage over Russia in the long term. For instance, although Russia spent a much higher percentage of its GDP on military expenditure, China’s 2017 military budget was more than three times higher than Russia’s. Furthermore, the sophistication of Chinese-made arms is increasing rapidly, and the number of China’s military personnel is also approximately two times larger than that of Russia. As a result, in any possible military partnership, Russia will be the junior partner, which the Kremlin will most likely find unacceptable.

ENGAGING AND RESTRAINING CHINA THROUGH MULTILATERAL ORGANIZATIONS

The Kremlin’s reluctance to accept a secondary role in China-Russia relations informs Moscow’s strategy toward multilateral institutions, through which the Russian government seeks to restrain Chinese influence. For instance, until 2017, the SCO included China and Russia, as well as Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. However, due to the size of its economy, China exercised outsized influence in the SCO. Therefore, to dilute Chinese power in the SCO, Russia advocated the inclusion of India, a long-term Russian partner, in the organization. Despite initial Chinese reservations, the SCO finally admitted India (and its rival Pakistan) as full members in 2017. Following India’s admission, its prime minister Narendra Modi sought to use
the SCO platform to criticize the Belt and Road Initiative and thwart other Chinese-led initiatives.\textsuperscript{97} Frustrated with disagreements within the SCO, the Chinese government is increasingly dealing with Central Asian countries bilaterally, instead of operating within the multilateral SCO framework.\textsuperscript{98} As a result, while Russia’s strategy of admitting India diluted Chinese power in the SCO, it also weakened China-Russia cooperation in Central Asia.\textsuperscript{99}

The desire to restrain China also motivated the Kremlin to create and play a leadership role in multilateral organizations that exclude China. To preserve Russia’s influence in Central Asia, Russia founded and strengthened its commitment to the EAEU, which comprises Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia.\textsuperscript{100} This customs union aims to preserve a domestic market for Russia, which comprised 85.7 percent of the EAEU’s combined GDP in 2018.\textsuperscript{101} Thus, the EAEU’s framework stands in stark contrast to the Belt and Road Initiative, through which Beijing hopes to improve connectivity between foreign and Chinese markets.\textsuperscript{102} Therefore, despite official statements about the union’s intentions to promote economic openness and foreign economic relations, the EAEU helps Russia maintain its economic dominance in the four former Soviet republics.\textsuperscript{103}

RELATIONS WITH OTHER ASIAN COUNTRIES

To avoid becoming a junior partner to China and to improve Russia’s negotiating position with China, Russia has sought closer ties with other Asian countries—most notably India, Japan, South Korea, and the Association of Southeast Asian Nations (ASEAN) countries like Singapore and Vietnam.\textsuperscript{105} For instance, Russia strengthened military ties with India and Vietnam, two countries that have territorial disputes with China.\textsuperscript{106} Since the early 2010s, Vietnam has sought to upgrade its military and naval capabilities in response to the People’s Liberation Army Navy’s growing assertiveness in the South China Sea.\textsuperscript{107} As part of Russia’s strategy to strengthen military ties with Asian...
countries and increase leverage with Beijing, Moscow signed a military cooperation agreement with Hanoi last year, which included provisions for joint Russia-Vietnam military drills, the deployment of a Russian boat for rescue operations in the South China Sea, and Vietnam’s purchase of Russian arms worth $1 billion.\(^{108}\) Due to the Kremlin’s recent efforts, Russia is currently the largest foreign source of Vietnamese military equipment, accounting for roughly 83.9 percent of Vietnam’s total arms imports between 2009 and 2019.\(^{109}\) Improved Russia-Vietnam security relationship not only allows Russia to find new markets for arms exports, but it also elevates Russia’s role in the South China Sea and increases Moscow’s bargaining power with Beijing.\(^{110}\)

In addition to Vietnam, Russia has also increased its military exports to India, which grew from around $0.6 billion in 2000 to approximately $4.0 billion in 2012.\(^{111}\) However, Russia-India arms trade declined to nearly $1.2 billion in 2019 as a result of growing defense ties between New Delhi and Washington.\(^{112}\) Nevertheless, Russia remains the largest source of military imports for India, which represents the second-largest importer of military equipment worldwide.\(^{113}\)

Despite Russia’s success in arms sales to Asian countries, its success in improving overall trade relations with Asian countries has been more limited. With only two Asian countries, China and South Korea, ranking among Russia’s top ten export markets, Europe still dominates Russia’s international trade relations.\(^{114}\) However, since 2014, Russia boosted its economic ties with South Korea, which ranked as Russia’s fifth-largest export market in 2018.\(^{115}\) As the world’s tenth-largest importer of energy, South Korea represents a crucial market for the resource-rich Siberia.\(^{116}\) In 2017, Russian commodity exports to South Korea amounted to $15 billion, which the South Korea government hopes will increase to $30 billion by 2020.\(^{117}\) Seoul also seeks to strengthen bilateral ties by signing a trade agreement with the Russian-led EAEU.\(^{118}\)
In addition to South Korea, Japan can play a key role in diversifying Russia’s Asian economic relations and accelerating the development of the Far Eastern region. In the early 2010s, Tokyo sought to improve ties with Moscow—Russian President Vladimir Putin and Japanese Prime Minister Shinzo Abe “met seven times over the period of 2013 and early 2014.” Japan also showed interest in the economic development of “the [Russian] Far East and trans-Baikal region” and provided 34 percent of the foreign investment inflows in those two regions in 2013. However, Russia-Japan economic ties suffered as a result of Japan’s decision to apply Western sanctions to Russia following the Ukraine crisis. Consequently, compared to Russia’s relations with China and South Korea, Russia-Japan economic ties remain weak.

Notwithstanding a trade agreement between Vietnam and EAEU, Russia remains a modest economic player in Vietnam and other ASEAN countries. Between 2005 and 2014, Russia’s trade with ASEAN countries increased five times. However, even after this five-fold increase, Russia-ASEAN trade in 2014 accounted for less than three percent of Russian international trade volume and “less than 1 percent of total ASEAN exports.” Between 2014 and 2018, Russia-ASEAN trade decreased from $22.5 billion to $19.9 billion, representing a 9.5 percent reduction. As a result, as of 2018, Russia-ASEAN trade volume remains lower than ASEAN’s total trade volume with Italy and Switzerland. Similarly, Russia’s role as a foreign investor in ASEAN remains modest—Russian foreign direct investment (FDI) accounted for less than 0.3 percent of total FDI inflows into ASEAN countries in 2017. Consequently, despite Russia’s pivot to Asia, Moscow’s economic presence in Southeast Asia remains modest at best.

CONCLUSION

Given China’s importance to the Russian economy and foreign policy, the success of Russia’s pivot to Asia will ultimately depend on China. Russia-China relations are based on three key issues—trade, military and security cooperation, and stability in Central Asia—each of which is likely to face challenges in the coming years. First, trade relations between Russia and China are skewed in China’s favor and will become increasingly so as the Chinese and Russian economy diverge in their performance. Second, with regard to arms sales, Russia will have increasingly less to offer as China becomes Russia’s competitor in high-tech military exports. Third, although Russia and China
now cooperate in the post-Soviet space, China is gradually replacing Russia as the primary source of trade and investment in the former Soviet countries. After surpassing Russia as the leading trade partner in all five Central Asian countries, Beijing is now expanding its presence even in countries that Russia considers to be within its sphere of influence. Considering Russia’s geopolitical sensitivities, China initially did not include countries like Georgia and Ukraine—which “have strained relations with Russia”—in the Belt and Road Initiative. Nevertheless, growing evidence suggests that China has been quietly making inroads even in those countries. For instance, in 2018, Georgia—which fought a brief war with Russia in 2008—signed a free trade agreement with China with the hope that Beijing will provide a counterweight to Moscow’s influence in Tbilisi. Beijing has also undertaken several construction projects in Georgia—like the Baku-Tbilisi-Kars railway line—which connects China with Armenia, Georgia, Iran, and Turkmenistan.

Against the backdrop of growing Chinese influence in former Soviet countries, Russia has mostly kept silent. Because of Russia’s strained relations with the West, Russia has limited leverage to voice its concerns against China. However, as the Kremlin increasingly realizes the extent to which Beijing has been expanding its influence at Russia’s expense, the Kremlin might seek to cooperate with Western partners to counteract Chinese influence there. In broader terms, as Moscow’s position relative to Beijing declines, it is unlikely that the Kremlin will accept the role of a junior partner, which Moscow has sought to avoid since the Soviet Union’s dissolution. Ultimately, this desire to avoid becoming China’s junior partner might drive the Kremlin to repair its strained relations with the United States and the European Union.

The author thanks Thomas Graham, distinguished fellow at the Council on Foreign Relations and former lecturer at the Yale MacMillan Center, for his advice and feedback in writing this paper.
Table A1. Russia as a recipient of Chinese investment, 2013 and 2018

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Investment (Billion $)</th>
<th>Percentage Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>United States</td>
<td>15.85</td>
<td>19.61%</td>
</tr>
<tr>
<td>2</td>
<td>Australia</td>
<td>8.58</td>
<td>10.62%</td>
</tr>
<tr>
<td>3</td>
<td>Britain</td>
<td>5.50</td>
<td>8.04%</td>
</tr>
<tr>
<td>4</td>
<td>Russia</td>
<td>6.25</td>
<td>7.79%</td>
</tr>
<tr>
<td>5</td>
<td>Kazakhstan</td>
<td>5.30</td>
<td>6.56%</td>
</tr>
<tr>
<td>6</td>
<td>Mozambique</td>
<td>4.71</td>
<td>5.83%</td>
</tr>
<tr>
<td>7</td>
<td>Egypt</td>
<td>3.60</td>
<td>4.45%</td>
</tr>
<tr>
<td>8</td>
<td>Malaysia</td>
<td>3.20</td>
<td>3.96%</td>
</tr>
<tr>
<td>9</td>
<td>Brazil</td>
<td>3.02</td>
<td>3.74%</td>
</tr>
<tr>
<td>10</td>
<td>Peru</td>
<td>2.89</td>
<td>3.58%</td>
</tr>
<tr>
<td>11</td>
<td>Uganda</td>
<td>2.18</td>
<td>2.70%</td>
</tr>
<tr>
<td>12</td>
<td>Angola</td>
<td>2.12</td>
<td>2.62%</td>
</tr>
<tr>
<td>13</td>
<td>Sierra Leone</td>
<td>1.70</td>
<td>2.10%</td>
</tr>
<tr>
<td>14</td>
<td>Pakistan</td>
<td>1.65</td>
<td>2.04%</td>
</tr>
<tr>
<td>15</td>
<td>Venezuela</td>
<td>1.40</td>
<td>1.73%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>80.81</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Investment (Billion $)</th>
<th>Percentage Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Germany</td>
<td>12.75</td>
<td>12.04%</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>9.68</td>
<td>9.14%</td>
</tr>
<tr>
<td>3</td>
<td>Britain</td>
<td>6.95</td>
<td>6.56%</td>
</tr>
<tr>
<td>4</td>
<td>Nigeria</td>
<td>6.54</td>
<td>6.18%</td>
</tr>
<tr>
<td>5</td>
<td>Chile</td>
<td>6.44</td>
<td>6.08%</td>
</tr>
<tr>
<td>6</td>
<td>Finland</td>
<td>5.66</td>
<td>5.35%</td>
</tr>
<tr>
<td>7</td>
<td>Canada</td>
<td>5.17</td>
<td>4.88%</td>
</tr>
<tr>
<td>8</td>
<td>France</td>
<td>4.84</td>
<td>4.57%</td>
</tr>
<tr>
<td>9</td>
<td>Bangladesh</td>
<td>3.66</td>
<td>3.46%</td>
</tr>
<tr>
<td>10</td>
<td>Peru</td>
<td>3.66</td>
<td>3.46%</td>
</tr>
<tr>
<td>11</td>
<td>Australia</td>
<td>3.16</td>
<td>2.98%</td>
</tr>
<tr>
<td>12</td>
<td>India</td>
<td>3.11</td>
<td>2.94%</td>
</tr>
<tr>
<td>13</td>
<td>Serbia</td>
<td>2.51</td>
<td>2.37%</td>
</tr>
<tr>
<td>14</td>
<td>Netherlands</td>
<td>2.42</td>
<td>2.29%</td>
</tr>
<tr>
<td>15</td>
<td>United Arab Emirates</td>
<td>2.23</td>
<td>2.11%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>105.88</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

Source: Author using data from the American Enterprise Institute and Heritage Foundation (2019) \(^{19}\)

ABOUT THE AUTHOR

Ryan Nabil is a master’s student at the Yale Jackson Institute for Global Affairs. He graduated from Kenyon College in 2015 with a B.A. in economics. Between 2015 and 2018, Ryan worked as an economic policy researcher at the American Enterprise Institute, where he published more than 40 articles in outlets including The Washington Post, U.S. News and World Report, and Foreign Affairs. At Yale, Ryan studies Chinese diplomacy in Europe, international relations, and comparative law.
ENDNOTES


6. Conversation with Thomas Graham, March/April 2019, Yale University, New Haven, CT.


8. See Sections “Trends in Chinese Investment in Russia” and “Trends in Russia-China Trade Relations.”


11. Ibid.

13. Conversation with Thomas Graham, March/April 2019, Yale University, New Haven, CT.

14. Ibid.

15. For a longer discussion, see Suslov, 1–11.


17. Suslov, 3.


20. Ibid., 1–11.

21. Ibid., 10.


27. Ibid.

28. Ibid.

30. Ibid., 3–7.

31. Ibid., 4.

32. Ibid., 3–7.


34. Ibid.


37. Dave, 7.

38. Gabuev, 3.


42. Eder, China-Russia Relations in Central Asia, 30–31.

43. Author’s analysis using data provided by the American Enterprise Institute (AEI) and Heritage Foundation, “China Global Investment Tracker (CGIT),”

44. Ibid.

45. Ibid.


51. Ibid.


54. Ibid.

55. Author’s analysis using data provided by AEI and Heritage Foundation, “China Global Investment Tracker.”


58. World Bank, “GDP (Constant 2010 US$).”

59. Ibid.


67. Ibid.


69. Lindsay Maizland, “China’s Modernizing Military”; also see Stockholm Institute of International Peace Research Institute, “New SIPRI Data Reveals

70. See Weitz, 29–35.

71. Ibid., 29–31.

72. Ibid., 30.


75. Medeiros and Chase, 8.


78. Ibid, 35.

79. Ibid.


81. Trenin, 9, 14–15; Artyom Lukin, 3.

82. Artyom Lukin, 5.

83. Ibid.


86. Artyom Lukin, 5.

87. Kotkin, 2.

88. Ibid.

89. Weitz, 30.


95. Ibid.

96. Ibid.


99. Ibid.

101. Author’s calculation using data provided by World Bank, “GDP (constant 2010 US$)”; also see Barbarshin, “The Eurasian Illusion.”


103. Ibid.


105. Conversation with Thomas Graham, March/April 2019, Yale University, New Haven, CT.


109. Author’s analysis using data provided by SIPRI, “TIV [Total Trend-Indicator Value] of Arms Exports from Russia.”

110. Medeiros and Chase, 11–12.

111. SIPRI, “TIV [Total Trend-Indicator Value] of Arms Exports from Russia.”


115. Ibid.


118. East Asia Forum, “Here Is Why South Korea May Be Turning to Russia.”

119. Artyom Lukin, 3.

120. Dave, 12.

121. Storey, 4–5.

122. Ibid.

123. Storey, 4–7.


125. Ibid.


127. Ibid.


129. Tsvetov, “Russia Still Seeking a Role in ASEAN”; Kapoor, “Russia and its Engagement with Southeast Asia.”
130. Weitz, 29–35.

131. Graham, “Russia Needs Options to Deal with China.”


135. Ibid.

136. Ibid.

137. See Graham, “Russia Needs Options to Deal with China.”

138. Ibid.

139. Author using data provided by AEI and Heritage Foundation, “China Global Investment Tracker (CGIT).”
BOOK REVIEW

THE SHANGHAI FREE TAXI AND LONG PEACE STREET

By Rana Mitter

Frank Langfitt, The Shanghai Free Taxi: Journeys with the Hustlers and Rebels of the New China (London, Weidenfeld and Nicolson)

Jonathan Chatwin, Long Peace Street: A walk in modern China (Manchester University Press)

For much of the 2000s, when foreigners discussed China, there was a gap between language and reality. Western correspondents, diplomats, and students wanted to make it clear to their compatriots that a changing China might be one of the biggest stories in the world. Yet there somehow didn’t seem to be a turning point—a moment that symbolized a shift to a world in which China really mattered to the rest of the globe. For visitors to China, the place seemed to be the same combination of anomalies that it had been since the 1990s—consumerist but authoritarian, prickly about its identity but keen to engage with the world. The peculiar mixture of pride and deference that marked China’s relationship with the world seemed destined to remain that way forever. “China keeps transitioning,” one frustrated journalist told me, “but it never seems to transition to anywhere.”

That time has come and gone. Whatever you may think of Xi Jinping’s China, it is definitively different from its predecessors—unapologetically illiberal and globally ambitious. This attitude did not begin with Xi. The 2008 global financial crisis led the Chinese leadership to doubt the relevance of a “Washington consensus” that had clearly failed to keep its own house in order. However, Xi’s rise to power from 2012 has heralded a new attitude both within China and in its relations with the wider world. I see its contradictions when I visit China and when I work with Chinese students in Britain. There is still a
great eagerness to learn in the Western world and an appreciation of the freedoms that are not available at home. Ironically, the one place on earth where it is impossible to write a critical academic study of China’s current leadership is... China. Yet there is also new confidence. Plenty of middle-class Chinese acknowledge and bemoan the rise in censorship and arbitrary exercise of legal power, as well as the constant political pressure in today’s China, which makes it much harder for professionals simply to keep their heads down and refuse to engage with politics. But even those who complain will, in some cases, echo one senior media figure who told me, in private: “Still, if there were an election, I would vote for Xi Jinping.” Recent uncomfortable evidence from democratic societies does suggest that there is no necessary gap between authoritarian personalities and high levels of popularity.

In times of fast change, well-informed accounts of what is happening in China have ever-greater value. To cover Beijing as a foreign correspondent is not the equivalent of working in Tokyo, New York, or London. Sources are afraid to talk to you, at least by name. The authorities take pride in trying to cut off reporters from stories and then complain that the “Western media” refuses to report China properly. China is a hardship post for journalists – although, like many such posts, it provides some of the most interesting stories imaginable. That reality makes books like journalist Frank Langfitt’s *The Shanghai Free Taxi*, and writer Jonathan Chatwin’s *Long Peace Street*, valuable and thoughtful reflections on a society that is changing fast and out of recognition.

Langfitt’s book is based on a wild idea that emerged to answer the question: in a country as constrained as China, how can you actually get close to ordinary people and ask their opinions? Langfitt, who served between 2011 and 2016 as the National Public Radio (NPR) correspondent in Beijing, decided to buy a car and operate it as a “free taxi.” He offered gratis rides in return for conversations about life in China. The book is a superb read; Langfitt has a real gift for narrative, and skilfully uses cliffhangers to keep the reader engaged. Among his passengers is Beer (his self-chosen Western name), a used-car salesman who lends that profession the same shining reputation in China it has gathered in the West. Beer tries to persuade Langfitt that he will be fired if he doesn’t buy the clunker that he is trying to push on the Westerner. Other riders in the book have rather higher motivations. His interviewee Johanna, who is a part of China’s growing professional middle class, epitomizes the
liberal sentiments that are so often hidden from the surface in China. She became aware of human rights law through the internet and studied it for two years in Sweden. Upon her return, she took on some of the toughest cases that modern China can supply, offering human rights assistance to people detained in Laogai labor camps or persecuted for practicing Christianity. Johanna’s story fits right in with what we know about the nature of the Chinese policing system behind the scenes. Activists are regularly arrested and harassed for seeking to exercise rights that are guaranteed under the Chinese constitution.

Another of the characters Langfitt delivers in his taxi sums up the ambiguities of modern China. Ashley is a young Chinese professional who emigrates to the United States. She is tired of the constraints of living in China. Yet she encounters the United States after the election of Donald Trump, and slowly but surely finds her assumptions about the West also fading. She meets Americans who are hostile to immigrants and have a limited sense of the advantages of democracy. Ashley still supports the idea of democracy, although Langfitt finds her “not completely convinced.” But when Langfitt asks her if China looks better once she had been overseas, she replies, “Definitely.”

Ashley is a telling example of how the calculus has changed on the contrast between China and the West. Many of the issues that China faces today are not really problems caused by the lack of democracy as such. Instead, as in many liberal societies, it is trust, however constituted, that has become a rare commodity. Some of the darker parts of Langfitt’s book concern a young woman searching for her missing sister; it appears that she has become caught up in a network of sex trafficking and drug use. Other characters find themselves caught up in financial scams, losing their life savings to swindlers in China, how can you actually get close to ordinary people and ask their opinions?
shiny-looking offices. None of these experiences is exclusive to China. But in the absence of a free media and open discussion, China’s modernization seems to contribute even further to a sense of existential lack of balance or stability. Langfitt’s book is marked by sensitivity—his “free taxi” clearly enabled him to develop relationships that are authentic and compelling, which makes the book a refreshing and necessary change from the increasingly shrill black-and-white contrasts that mark much of U.S.-China relations.

Jonathan Chatwin’s book contrasts nicely with Langfitt’s, in that it has a much narrower geographical focus. It takes place on one street in Beijing but has a much longer historical backstory. Chatwin sets aside two days to walk along Chang’an Avenue, “Long Peace Street,” the arterial road that cuts west-east through the Chinese capital, with its center at Tian’anmen Square. If Langfitt’s book puts an unease about the face of contemporary China at its heart, Chatwin’s is shaped by a melancholy about the disappearing past. Ghosts make their way through the book on a regular basis. One powerful section on the Babaoshan cemetery, where the heroes of the Communist revolution are laid, expresses that absence well. Peng Dehuai, the great general who fought alongside Mao in the CCP’s rise to power, was exiled after confronting Mao over the horrors of the Great Leap Forward, then died during the latter years of the Cultural Revolution. Yet his ashes were not originally laid to rest in the heroes’ cemetery; that did not happen until after the repudiation of the Cultural Revolution under Mao’s successors. But in an ironic coda, the ashes were then moved again so that Peng could be reburied in his native province. Another “ghost” that appears in the book is the Shougang (Capital Steel) plant that once stood at the western end of the avenue. As China abandoned its dreams of a command economy and plunged into the market, this once-proud set of furnaces—which also included restaurants, nurseries, and clinics, the cradle-to-grave provision associated with the Chi-

The overwhelming sense that comes from Chatwin’s portrait of Beijing is of constant renewal: a renewal where the past is not just forgotten, but often deliberately obliterated.
inese “work unit”—was abandoned. The overwhelming sense that comes from Chatwin’s portrait of Beijing is of constant renewal: a renewal where the past is not just forgotten, but often deliberately obliterated. Chatwin’s humane, gentle prose makes him the ideal companion to poke around the back alleys along the route and remind us of a Beijing that existed just a few decades ago. Indeed, visitors to the capital could take the book with them as they make part of the walk themselves.

These books are written in the context of the 2010s. What aspects of the 2020s can one see nestling in their descriptions of today’s China? Probably the single most important element is the growing sense of technology as the most transformative factor in the country today. As China moves down the path to becoming a society where the government collects huge amounts of data with little if any expectation of privacy from its citizens, all of whom operate their lives from their smartphones, many of the interstitial spaces found by both Langfitt and Chatwin seem set to disappear. These two books are excellent examples of how today’s China still has spaces where frank discussion of the present and reflection on the past is possible and necessary. Let us hope that such books can still be written 10, 20, and 50 years into the future.

ABOUT THE AUTHOR

Rana Mitter is the current Director of the University China Centre at Oxford University. He is the author of several books including Modern China: A Very Short Introduction (2008, new ed. 2016) and the award-winning A Bitter Revolution: China’s Struggle with the Modern World (2004). His most recent book China’s War with Japan, 1937-45: The Struggle for Survival (U.S. title: Forgotten Ally) was named a 2013 Book of the Year in the Financial Times and the Economist, was named a 2014 CHOICE Outstanding Academic Title and won the 2014 RUSI/Duke of Westminster’s Medal for Military Literature. He is Professor of the History and Politics of Modern China at Oxford University.
Op-Ed

Why Peace Corps Should Stay in China

By Krista Mangiardi

Given the Peace Corps’s crucial importance to international cultural exchange, it is a mistake to close the program in China. On January 16, 2020, Senator Marco Rubio (R-FL) released a statement, before any press release from the Peace Corps, praising the closure because “China is no longer a developing country.” Volunteers on the ground were shocked by the Senator’s statement. Later that day, the 130 Peace Corps volunteers in China, all of whom are English teachers, learned that the program would
close sometime in 2021. Two weeks later, they evacuated due to the spread of COVID-19 and the program closed immediately.²

Sen. Rubio’s statement suggests that the Peace Corps made an internal decision to close the program. Eventually, the Peace Corps released a statement stating they would phase out the program given “many significant changes in China.”³ Over time, however, a much more complicated truth has emerged, involving a National Security Council meeting chaired by Deputy National Security Advisor Matthew Pottinger.⁴ It appears that mounting political pressure and U.S.-China tensions contributed to the decision to close the program.⁵

From 2017-2019, I served as a Peace Corps volunteer in Gansu, China. Having been on the ground, I believe that whether the closure is due to China’s development or to escalating U.S.-China tensions, the program should continue.

Slashing a long-established program that improves U.S.-China understanding is dangerous at a time of heightened bilateral tensions. Senator Rubio is not necessarily wrong to suggest China is no longer a developing country. The Peace Corps, however, is the wrong target. Only one part of its mission relates to development work. The Peace Corps should remain in China to fulfill its two other goals: “to help promote a better understanding of Americans on the part of the peoples served” and “to help promote a better understanding of other peoples on the part of Americans.”⁶ These aims are important, especially in times of disagreement and heightened bilateral tensions.

Compared to similar programs, the Peace Corps is a cost-effective way to improve American understanding in other regions. In the 2019 fiscal year, the Peace Corps China program cost taxpayers only $4.1 million.⁷ In comparison, the U.S. Agency for Global Media spends over $12 million each year on news broadcasting in Cuba, another country deemed “hostile” to U.S. in-
Each of the 130 volunteers in China this year taught and interacted with hundreds of students and teachers each year, achieving its strategic goals at a low cost.

The Peace Corps helps Chinese citizens to develop a sophisticated understanding of the United States beyond the state-controlled media narrative. For instance, consider the average person in a rural Guizhou village who cannot afford to travel abroad. A Peace Corps volunteer is often the first American that a person in rural China ever meets. Volunteers do not just teach English: they share stories about American culture, screen films, and provide a human face to a far-away country. It is in the U.S. interest for the 41 percent of the Chinese population living in rural areas to understand Americans beyond government officials, movie personalities, and others portrayed in Chinese media. Truly strong and strategic foreign policy is culturally-informed. Over 350,000 Chinese students currently study in U.S. colleges and universities. Yet, in the 2017-2018 academic year, only about 12,000 American students studied in China. Future Chinese leaders surge ahead in this area, understanding the United States better than many future U.S. leaders understand China. Even President Xi sent his daughter to study in the United States. He is not alone among Chinese leaders. Given China’s importance to the international order, the United States needs leaders who speak Mandarin Chinese, understand Chinese communication styles and cultural values, and have traveled to regions of China outside of Beijing and Shanghai. Peace Corps volunteers not only help the average Chinese citizen learn about the United States, but also gain invaluable experience in China. Many return to the United States and use this knowledge in global careers.

Why should policymakers use the Peace Corps to address the critical lack of American expertise in China? In addition to its low cost, it allows for deep
and long-term community immersion, which is rare in international exchange programs. This is especially true in the least developed parts of China, such as the province in which I served. Peace Corps volunteers serve for two years at local living standards, supporting themselves on a modest stipend. This allows for interpersonal exchange not possible in short-term teaching contracts or study abroad programs, which send Americans to major Chinese cities.

Peace Corps volunteers do impactful work teaching English, sharing American culture, and learning about China all at the same time. Given that the U.S.-China relationship is critical to international relations, even Senator Rubio should recognize the need for a more nuanced understanding of China and Chinese culture. The U.S. government should bring the Peace Corps back to China.

2009-201 Peace Corps Volunteers play Mahjong with their Chinese students. Photo by U.S. Peace Corps.
ABOUT THE AUTHOR

Krista Mangiardi is a master’s student at the Yale Jackson Institute for Global Affairs. She graduated from Hampshire College in Amherst, MA with a B.A. in liberal arts and a certification in Teaching English to Speakers of Other Languages. At Hampshire, she concentrated her studies in journalism, literature, and cultural studies. She served as a Peace Corps volunteer in Gansu, China from 2017-2019. At Yale, Krista studies U.S. foreign policy with a focus on diplomacy and China.

ENDNOTES


3. Ibid.


INVESTMENT SCREENING FOR DEVELOPING ASIA

By Aaron Baum

INTRODUCTION

Brazilian farmer Edimilson Santana told The New York Times in 2011 that Chinese consumers are buying up “more [soy] than anyone… This could be a new beginning for farmers here.”¹ But where Edimilson saw opportunity in a $7 billion deal to supply six million tons of soybeans per year to China, others saw risks to the country’s sovereignty and national security. When local officials refused to sell Chinese investors the massive tracts of land they sought, China chose instead to provide credit to farmers to expand soybean production.² But even this solution left some concerned about Brazilian food security and overreliance on China as a trading partner, leading Brazil’s Attorney General Luís Inácio Adams to issue a new interpretation of a 1971 law that tightened restrictions on foreign ownership of Brazilian land.² Chinese investment in Brazil has fallen substantially since then, with some pointing to an unfair targeting of Chinese agribusiness and even accusations of Sinophobia.⁴

That struggle between growth and security is playing out across the developing world. In most cases, developing countries with few comparative advantages to offer multinational firms are wary to do anything that restricts foreign direct investment (FDI). Meanwhile, developed countries have realized that they cannot protect their own critical industries if countries with which they regularly trade are vulnerable to intrusion themselves. The U.S. Congress, for instance, resolved in the most recent reforms to the United States’ investment screening mechanism to exchange information with U.S. partners with respect to investment and technology that could threaten the national security of the United States or its partners.⁵ This is of particular priority to the United States as Huawei equipment finds a home in more and more countries. As Vice President Mike Pence said, “we’ve urged our allies around the

Buildings in Beijing. Photo by Zhang Kaiyv.
world to build secure 5G networks that don’t give Beijing control of our most sensitive infrastructure and data as well.\textsuperscript{6}

But though the United States may wish for developing economies to mimic their own investment screening policies, the emerging Asian economies that make up the Association of Southeast Asian Nations (ASEAN) face different threats from Chinese investment and must create policies that best protect against those unique threats. In most cases, the government of the People’s Republic of China (PRC) is not targeting quantum computing or semiconductors in ASEAN, but rather is looking to acquire critical infrastructure, resources, or data.\textsuperscript{7} ASEAN must also balance economic growth and national security more carefully than developed countries that worry less often about FDI.

This paper recommends that ASEAN countries create investment screening mechanisms close to OECD recommendations and that ASEAN itself encourages working- and Ministerial-level engagement on investment screening via a new Sectoral Ministerial Body that will track regional investment trends. Importantly, they should take these steps sooner rather than later to preempt, rather than react to, a national security crisis.

**CASE STUDY: HOW CFIUS SCREENS INVESTMENT**

The most recent Annual Report from the United States’ investment screening mechanism, the Committee on Foreign Investment in the United States (CFIUS), outlines a number of national security factors that the body considers, including transactions that involve: defense or military, dual-use technologies (including network and data security, semiconductors, and biotechnology), government contracts related to national security, critical infrastructure (including energy, transportation, and finance), “loss in U.S. technological competitiveness,” and personally identifiable information (PII).\textsuperscript{8} Across all of these transactions, CFIUS evaluates risk to U.S. national security as a function of threat — “whether a foreign person has the capability or intention to exploit or cause harm” — and vulnerability — “whether the nature of the U.S. business, or its relationship to a weakness or shortcoming in a system, entity, or structure, creates susceptibility to impairment of U.S. national security.”\textsuperscript{9}
National security is, admittedly, a vague term. Legendary political scientist Harold Lasswell defined national security as “freedom from foreign dictation.” That definition is tempting to use in the context of investment security given that foreign control of a particularly sensitive or critical business could threaten national security without that business touching on defense directly. The term’s vagueness could also itself be a feature, as various legal experts have commented that CFIUS legislation has intentionally avoided defining national security to allow the body to “respond to novel or emerging threats.” This tactic may be less useful for developing countries, which ought to instead prioritize clarity and transparency in investment screening in order to balance protecting national security and promoting investment.

Examples of areas that CFIUS screens will be more helpful than these academic definitions for practical implementation of investment screening. Moreover, the actual practice of CFIUS is much more restricted than the vague academic definitions would suggest:

**PII:** Reports that CFIUS forced the Chinese firm Kunlun Tech to sell gay dating app Grindr (an American firm sold to Kunlun that had avoided initial CFIUS review) demonstrate how CFIUS reviews sensitive data transactions. Though CFIUS deliberations are kept secret, anonymous sources report that CFIUS is concerned about PII for its potential abuse by foreign intelligence services. Of Grindr’s over three million users, some are likely national security officials, and there is evidence that the PRC has both the capability and motivation to mine data on American leaders and other security clearance holders.

**Energy:** Energy is a crucial aspect of national security—it powers hospitals, military communications, air control, and more. Russia’s control of Europe’s gas supply demonstrates the danger of entrusting stable supply of that energy to a foreign country, particularly one in which business decisions are tied closely to geopolitical considerations. In the dead of winter 2009, 10 died of cold in Poland as Russia and Ukraine failed to come to an agreement on continuing to deliver gas across the EU. Though these gas crises pop up every few years, the EU has still failed to end its reliance on Russian gas.

**Emerging Technologies:** The U.S. Bureau of Industry and Security issued guidance that lists general categories of emerging and frontier technologies essen-
tial to national security. But CFIUS is not merely concerned with the “dual-use” nature of these technologies—that they can be used for both civilian and military purposes—the body also considers U.S. “technological leadership” as an aspect of national security. As the Treasury Department expressed in a letter to U.S. semiconductor company Qualcomm and its proposed Singaporean acquirer Broadcom, “the weakening of Qualcomm’s position would leave an opening for China to expand its influence on the 5G standard-setting process.” CFIUS was worried that Broadcom would cut Qualcomm’s leading research & development spending, which “could result in a weakening of Qualcomm’s technological leadership.”

CHINA’S “GOING OUT” STRATEGY

In sum, CFIUS covers a broad range of industries and generally remains constrained by its statutory mandate to only consider a transaction’s impact on national security specifically. And though CFIUS is by law “non-discriminatory,” it seems to disproportionately review Chinese acquisitions. Four of five total blocks using Exon-Florio authority targeted proposed acquisitions by Chinese firms (the fifth block was the Qualcomm-Broadcom transaction, which as explained above also had a China nexus), and a recent Congressional Research Service report even acknowledged that CFIUS’s role has evolved primarily in response to the growing influence of “China and state-led firms.” But Chinese firms are not the only ones that represent national security threats. Rather, this focus on China is due to the role of investment screening mechanisms as measures of “last resort” and the PRC’s unique state-directed outbound investment.

Investment review mechanisms are not the only ways that countries restrict inbound FDI. Rather, they are the “last resort” to block a transaction that threatens national security but is legal under the rest of the nation’s investment laws. If a nation identifies a sector critical to the national interest regardless of the nationality or motivations of the acquirer, that country can restrict all transactions in that sector. Looking at these restrictions through the “threat + vulnerability = risk” model, these sector-specific restrictions mostly protect “vulnerabilities.”

On the other hand, a screening mechanism that requires filings for proposed deals across all sectors can block transactions by considering a full under-
standing of the vulnerabilities and threats involved. Thus, investment screening is better suited for restricting transactions from a country that represents a threat: one acting to undermine a target country’s national security that may even attempt to avoid traditional foreign investment restrictions (indeed, recent changes to CFIUS extend coverage to transactions “designed or intended to evade or circumvent” CFIUS review). The PRC represents such a threat, having demonstrated the intent and capability to use business as a foreign policy and security tool. The U.S. government has released a number of reports evaluating the PRC’s “economic aggression,” which focus mainly on the PRC’s attempts to transfer technology and intellectual property in support of their military.

In 1999, the Chinese Communist Party (CPC) announced the “Going Out” strategy to support Chinese firms making investments abroad by leveraging the country’s massive reserve of foreign currency. The original stated objective of the program was to support the export of Chinese goods, but since then the PRC has increasingly subsidized and encouraged firms making geostrategic investments meant to transfer technology from target countries to China. A document from China’s Ministry of Commerce lists “‘Going Out’ for the purpose of obtaining technology” as one of four strategic directions for the program, and a Ministry of Commerce official argued more recently that “acquiring new international technologies” is one of four reasons that China today boasts a number of large firms that have decided to invest abroad. The strategy was successful, with Chinese investors participating in 16 percent of overall U.S. venture capital deal value in 2015, before the CFIUS crackdown.
The PRC’s Military-Civil Fusion strategy, explained in the State Council’s “Long-term Scientific and Technological Development Plan for 2006-2020,” calls for civilian researchers to work closely with military authorities to find defense uses for civilian research. The strategy calls for acquiring and integrating foreign scientific research and technology as well: “Strengthening the digestion, absorption and re-innovation of imported technologies.” And while the PRC has had to rely on small acquisitions of early-stage dual-use technology acquisition in the United States to avoid CFIUS scrutiny, it has imported billions of dollars in advanced military technology from the EU through legal, quasi-legal, and illegal means.

**COULD INVESTMENT SCREENING BE USEFUL FOR ASEAN?**

This paper’s discussion of investment screening in the United States showed that a mechanism to review inbound investments for their national security implications can be a useful tool to protect against economic aggression from a malign actor threatening a country’s national security. ASEAN certainly faces this threat from China. Though the region can learn from CFIUS, the priorities and thus statutory guidance for mechanisms in developing countries ought to look different from the U.S. model. ASEAN faces different threats than the United States due to its role as China’s security “backyard” rather than target for advanced technology acquisition, and the region must protect different industries given its developing rather than developed status. Broadly, investment screening would be a useful tool for ASEAN nations to protect their national security in critical infrastructure, critical resources, PII, and telecommunications.

Even before China fully emerged onto the global stage in 2008 and the West began attacking Chinese economic foreign policy more recently, some academics observed that China used business and economic policy to pursue foreign policy objectives and its security interests in Southeast Asia. Indeed, some argue that China’s economic engagement with ASEAN, including the ASEAN–China Free Trade Area signed in 2002, is primarily motivated by the PRC’s security imperative to encourage Southeast Asian nations to bandwagon with China’s ascent to regional hegemon under Hu Jintao’s “peaceful rise” strategy. The PRC moreover has an incentive to “defuse American influence [and secure] key markets and raw materials needed for China’s economic security.”
These nations’ security outlook also differs from the United States due to their shared regional security challenges. Barry Buzan and Ole Wæver’s *regional security complex theory* argues that “since most threats travel more easily over short distances than over long ones, security interdependence is normally patterned into regionally based clusters,” particularly for lesser powers like the ASEAN states.²⁸ Historical (decolonization in Southeast Asia, the Vietnam War, etc.), cultural (religious diversity, ethnic tensions, etc.), and geographic (shared security obligations in the South China Sea, importance of the Malacca Strait, etc.) factors have contributed to the formation of what Buzan and Wæver call the Southeast Asian Regional Security Complex (RSC).²⁹

The following examples demonstrate the threats and vulnerabilities that foreign investment screening mechanisms in ASEAN could help mitigate:

**Critical Infrastructure**: The PRC has demonstrated its regional security interests through incursions into the South China Sea and economic aggression via the “String of Pearls.” A PRC State Council white paper from 2015 makes official the gradual expansion of China’s understanding of its regional interests in the Indian Ocean Region (IOR) by arguing for a novel concept of “frontier defense” that justifies “warfighting into the global commons” contrary to the traditional “homeland-based defense posture.”³⁰

An important component of this strategy is China’s Maritime Silk Road, a strategy to acquire stakes in ports and other critical infrastructure throughout Asia.³¹ Though ostensibly commercial investments, a classified report for the U.S. Department of Defense proposed the “String of Pearls” theory, which argues that China is planning to build naval bases across the IOR.³² A Congressional review concluded that “Chinese investments in commercial ports in the Indian Ocean and Chinese naval diplomacy with countries in the region probably will improve the [People’s Liberation Army Navy’s (PLAN’s)] ability to replenish using regional ports and could lay the groundwork for future logistics hubs in the Indian Ocean.”³³ Regional experts, like the National University of Singapore’s Archana Atmakuri, express similar concerns: “The port development projects… are all happening in India’s backyard, and this feeds into China’s encirclement strategy towards India.”³⁴ The PLAN has made dozens of port calls in the IOR in recent years, and an ability to militarize commercial investments would significantly extend PLA force projection and be a major asset in a South China Sea or other maritime IOR conflict.
While the full national security ramifications of this ownership are still unclear, the example of the Dubai Ports World (DP World) controversy demonstrates some potential threats to national security even outside of maritime conflict and ownership by an overtly malign entity. In 2006, state-owned Dubai firm DP World withdrew from a deal to manage operations at six U.S. ports on concerns from lawmakers that ownership by Dubai, with its lenient export restrictions and history as a transfer point for illicit nuclear technology, could make the American ports into hubs for terrorist and other illegal proliferation networks.\(^{35}\)

A notable example of port control in ASEAN is Chinese state-owned investment company CITIC Group leading two consortia that won bids to build a deep-sea port and industrial park in Myanmar’s Kyaukpyu Special Economic Zone, ending up with a 70 percent ownership stake in the port in an agreement with the country.\(^{36}\) This project, and the now famous Hambantota port in Sri Lanka, demonstrate another strategic vulnerability in ASEAN—unsustainable debt.\(^{37}\) Though sovereign debt in most cases falls under “national interest” rather than “national security,” the PRC may be able to leverage its role as a creditor over desperate debtors and compel them to make concessions friendly to China’s geopolitical and security interests. For instance, the debt-to-equity swap in Hambantota gave China control over the port and a potential foothold in the IOR, and in other cases China could leverage debt to convince countries to cut off relations with Taiwan or make concessions in the South China Sea. Even if merely a “national interest” question, public indebtedness is a trend reaching crisis levels in ASEAN that would regardless merit at least macro analysis by a multilateral investment review mechanism.\(^{38}\)

\textit{Natural Resources}: China’s near monopoly over rare earth metals is a telling case study in how the PRC uses natural resource investments for strategic benefit.
benefit. Rare earth metals are a vital input for an array of civil and military technologies—from smart phones and medical devices to submarines and guided missiles—but the world first became worried about China’s control in 2010 when the PRC threatened to cut off supplies to Japan following an incident near disputed islands in the East China Sea. That threat was a “wake up call” to the world that it must diversify supplies of rare earth metals in order to protect global security.\textsuperscript{39} Though China’s share of the global rare earth supply has fallen since then from 97 percent to 70 percent, the PRC continues to use its dominance as a cudgel in disputes (most notably the U.S.-China Trade War).\textsuperscript{40}

The PRC leveraged poor FDI restrictions to establish early dominance in rare earths, and may return that investment strategy if its market share continues to slip. An example: the U.S. firm Magnaquench, which produced rare earth magnets for General Motors cars, was acquired by a Chinese firm in 1995 following a review by the U.S. government and an agreement to maintain U.S. operations for five years. As soon as the five year period expired, the Chinese owners shuttered American operations and moved the entire business, along with its tech, to China. This FDI approach was “the Chinese modus operandi with respect to controlling the [rare earth] industry.”\textsuperscript{41} Today, the only major non-Chinese rare earth processing plant is the Lynas facility in Malaysia, owned by the Australian rare earth mining firm Lynas Corporation.\textsuperscript{42} This plant, often cited as critical to the global effort to reduce Chinese rare earth control, has previously been threatened with Chinese acquisition, and may be threatened again without legal safeguards. Indeed, the last time a Chinese firm tried acquiring a substantial share of Lynas Corporation, the company withdrew the proposal citing strict requirements by Australia’s Foreign Investment Review Board. Since then, a noted Australian economics commentator recommended that Australia invite Chinese investment into their rare earth sector, encouraging the Review Board to this time “remain open” to the prospect.\textsuperscript{43}

China is extracting natural resources across the developing world, particularly in ASEAN where it can cheaply transport the materials to mainland China for processing. The example of rare earth minerals demonstrates how the PRC can use that investment to produce both vertical and horizontal integration which can then threaten the stability of global supply chains.
**PII and Telecommunications:** This paper will only briefly touch on Southeast Asia’s private data and telecommunications vulnerabilities, as these are broadly similar to the vulnerabilities in developed countries. On PII, Southeast Asia holds a massive trove of exploitable data given the region’s above average penetration rates for social media and internet usage, particularly amongst other developing countries. As in the United States, Chinese money is aggressively looking to acquire startups in Southeast Asia. Unlike in the United States, most ASEAN countries have no CFIUS-style mechanism to review this proliferation of deals. In telecommunications, China’s 5G champion Huawei has long provided most telecommunications services to Southeast Asian nations, even as the United States continues to accuse the company of providing the PRC with a backdoor into the infrastructure that the company builds. These sectors are important to acknowledge as potential vulnerabilities because they demonstrate China’s ability to intrude across a range of sectors (PII is a concern in almost any consumer internet company), and thus provide a strong basis for an investment review mechanism that can similarly cover transactions not with respect to sector, but instead solely focused on national security risk.

**DOMESTIC RECOMMENDATIONS**

ASEAN nations face more vulnerabilities from more actors than are listed above. Indeed, developing countries around the world have been forced to make trade-offs between economic growth, national security, and even sovereignty as they seek to escape the middle-income trap. Multinational enterprises choose countries for FDI based on holistic cost-benefit analyses, which include trade costs and overall investment restrictiveness. As a result, developing countries with little knowledge or capital to offer investors instead pursue a race to the bottom, particularly in search of easy money from state-directed investors that comes with few up-front strings attached (but potential long-term strategic consequences). That hunger for FDI leaves nations vulnerable to economic aggression and exploitation. And while investment screening has traditionally been seen as the realm of developed countries for that reason these measures can protect national security while continuing to demonstrate openness to FDI if implemented carefully.

The methodology for the OECD’s FDI Restrictiveness Index referenced notes that “measures taken for reasons of public order and essential security inter-
ests... are not scored.” Thus, these countries will likely not be penalized in global measures of restrictiveness if they implement measures solely aimed at protecting national security. To do so, these nations must carefully follow international best practices and signal the implications of any new investment screening mechanisms in order to avoid scaring off international investors. In 2009, the OECD Council adopted four broad “Guidelines for Recipient Country Investment Policies Relating to National Security”: (1) non-discrimination, (2) transparency and predictability, (3) regulatory proportionality, and (4) accountability. Most existing investment screening mechanisms have been successful at the latter two but unsuccessful at the former, but those implementation questions matter less for countries which do not struggle to attract FDI such as the United States, Canada, and Australia. If a mechanism in Indonesia or Malaysia operated with the same secrecy as CFIUS, however, it may become difficult to attract international investors. Thus, the mechanisms of ASEAN should adopt the OECD recommendation to disclose investment policy actions, which CFIUS rarely does. These countries should also publish their justifications for clearing or blocking transactions, which CFIUS never does.

One interesting model for promoting transparency and ease of filing is India’s new Foreign Investment Facilitation Portal, which replaced the country’s Foreign Investment Promotion Board in 2017 and decentralized its powers from a central screening mechanism down to the relevant Ministries or Departments. CFIUS filing is time-consuming, opaque, and expensive for international investors, who generally hire expensive law firms experienced in the ins-and-outs of the secretive process. Southeast Asian nations may want to adopt a mechanism closer to the expedited review process that India decided on in order to impose fewer burdens on potential investors.

On non-discrimination, it is easier for the United States, which has labeled China a strategic competitor, to merely feign non-discrimination while primarily targeting transactions from China. ASEAN, however, is understandably reticent to adopt a new investment restriction traditionally used in the West to target Chinese acquisitions given the region’s reliance on Chinese investment. New screening mechanisms must thus engage with Chinese investors on a collaborative basis and show that they will still allow for Chinese investments that are demonstrated to not endanger national security. Clearly
differentiating these mechanisms from the temptations of some U.S. foreign policy advisers to end the non-discriminatory nature of CFIUS may even help to attract more international investors worried that their investments would be reviewed arbitrarily and based on potentially discriminatory factors in other countries. This is because discrimination against all China-linked investments will not only impact investments from Chinese firms, but will also dissuade other foreign investors that may do business with Chinese firms or may themselves have some Chinese investors. Not all of these actors are malign.

But as acknowledged in the analysis of Southeast Asia’s critical infrastructure and resources, the threats to national and economic security do not end at the borders of these countries. An investment in one could threaten the security of another. For that reason, multilateral engagement on investment screening is also crucial to protecting the security of ASEAN.

MULTILATERAL RECOMMENDATIONS

ASEAN ought to establish a new Sectoral Ministerial Body within the ASEAN Political-Security Community that functions throughout the year at the working level and meets annually at the Ministerial level to (1) monitor trends in FDI and investment security; (2) review, discuss, and—in the case of a true emergency—issue recommendations on individual transactions that could compromise regional security; (3) create networks for intelligence sharing to support the work of national-level investment screening mechanisms; and (4) share best practices for investment screening and issue recommendations à la the OECD “Guidelines for Recipient Country Investment Policies Relating to National Security.” These recommendations closely mirror the new EU framework for investment screening that leaves enforcement decisions up to sovereign nations but unites Europe in a regional understanding of economic security. This body should be organized at the ASEAN level, rather than through APEC, ADMM-Plus, etc. level because the sensitive nature of investment screening guidelines and recommendations should be controlled by the group of ASEAN countries alone—at least initially. This is particularly important given China’s influential role in Asia’s other multilateral organizations.

Buzan and Wæver point out that the Southeast Asian RSC is unique for its juxtaposition of superpower intervention (whether from China or the United
States) with a multipolar regional security structure represented in ASEAN. The region, then, is perfect for a multilateral investment screening mechanism: a large power, China, which has demonstrated interest in regional security dominance through its aggression in the South China Sea and IOR, can be effectively countered through cooperation of smaller powers. That mission is appropriate for the small regional body of ASEAN rather than larger global forums because, as Buzan and Wæver explain, the countries face unique regional security threats. Unlike in Europe, where “the regional dynamic subordinated to the global one” as a consequence of the importance of the region to Cold War competition, the Southeast Asian RSC has been “heavily penetrated by the global level, but not overlaid by it.”

Thus, unique regional dynamics, threats, and security issues remain in Southeast Asia that can be addressed through cooperation.

Few if any of the purported doomsday scenarios of Chinese investment have come to pass. Yes, there has been substantial IP theft and transfer from the U.S., but the PRC has not shut down the American power grid or parked aircraft carriers at Hambantota. But this is the nature of security problems. A billion-dollar missile defense system is only useful when missiles are raining down, but it is at precisely that moment when the billion-dollar investment becomes invaluable. However, even if ASEAN does not believe that China, or any other country or foreign actor, has malign intent and would utilize strategic investments to impair a nation’s national security, the question is still at least worth study.

In the 302 page “2019 ASEAN Investment Report” co-published by the ASEAN Secretariat and the United Nations Conference on Trade and Development (UNCTAD), security considerations were given only a couple brief mentions (less than a sentence) in the context of data privacy. In contrast, the yearly UNCTAD World Investment Report dedicates a section to “National Investment Policy.” That section in this year’s report began with: “New investment restrictions or regulations for foreign investors were mainly based on national security concerns about foreign ownership of critical infrastructure, core technologies, elements of the defense sector, sensitive business assets or residential property.” As this quote demonstrates, investment security is a growing global priority, and ASEAN ought to at least track the threats it faces, if not mitigate them. CFIUS, as discussed earlier, was originally estab-
lished with no authority to block or even review individual transactions, but to merely report on developments on foreign investment in the United States.

One particular benefit of such a multilateral monitoring measure would be to protect regional security that might otherwise suffer from a collective action problem and negative externalities. In the case of certain critical infrastructure and raw materials, a purely domestic analysis of national security risks would not account for potential global security implications. For instance, an Indonesian review mechanism could very reasonably conclude that a Chinese state-owned enterprise’s acquisition of a majority stake in a firm managing port security at the busy Port of Tanjung Priok does not represent a threat to their national security. However, that transaction taken in the context of dozens of other Chinese transactions around ports in the IOR could build up the influence that the PLAN needs to project force in the region. And even if Indonesia does not mind Chinese incursions, other regional partners do. Similarly, Malaysia or Australia allowing a Chinese firm to purchase the Lynas rare earths processing plant would represent a significant blow to global economic security by allowing China to tighten its monopoly on rare earth production, but may not threaten Malaysia’s security (particularly if the two countries come to an agreement on supply assurance of rare earths for Malaysia’s domestic needs).

ASEAN cannot and should not create any supranational investment screening system that would violate state sovereignty. ASEAN states make decisions all the time that are counter to their national or global security, and that is entirely their prerogative. But a body that could at least issue recommendations and analysis or create a system for information sharing could help those countries understand whether they should begin making steps in the direction of protecting their national security against emerging economic threats.

CONCLUSION

With the developed world now waking up to the threats to national security from foreign investment, developing countries have the unique opportunity to learn from their mistakes and preemptively mitigate risks before it is too late. The EU, a much tighter integrated and economically secure group of states, only recently adopted unified investment screening, so admittedly it may be some time before ASEAN comes around. Thus, important future steps
for research will be how the West can best engage these hesitant developing countries on investment screening. At the end of the day, these countries may simply say that they cannot afford to lose any investment, let alone the massive pots of money provided by the PRC. Thus, another next research step will be to evaluate methods for other developed countries to replace China as an influential investor and supporter for the developing world. Regardless, economic security will only become a greater concern as global conflicts are increasingly waged not on the battlefield, but in the boardroom.

ABOUT THE AUTHOR

Aaron Baum is a senior at Georgetown University majoring in East Asian business and politics and pursuing the honors certificate in international business diplomacy. He is a 2018-2019 student fellow in the Initiative for U.S.-China Dialogue on Global Issues Student Fellows program. Currently, he is the editor-in-chief of the Georgetown Journal of International Affairs.

ENDNOTES


2. Ibid.


15. These technologies include: biotechnology; artificial intelligence; position, navigation, and timing (PNT) technology; microprocessor technology; advanced computing technology; data analytics technology; quantum technology; logistics technology;


18. These restrictions include caps on foreign ownership (e.g., less than 50 percent), legalized state monopolies, constraints on foreign personnel or operations, and even informal measures like opaque and slow procedural requirements. Media, transport, real estate, and fisheries are heavily restricted worldwide. See, Stephen Thomsen and Fernando Mistura, “Is investment protectionism on the rise?”, Organization for Economic Cooperation and Development, 2017, http://www.oecd.org/investment/globalforum/2017-GFII-Background-Note-Is-investment-protectionism-on-the-rise.pdf.


29. Ibid., 128-29.


program/hambantota-chittagong-and-the-maldives-unlikely-pearls-for-the-chinese-navy/.


48. While national security as it relates to FDI remains an understudied area, there is substantial literature proving that developing countries race to the bottom to create comparative advantages in other areas, such as cost of labor. For evidence of Chinese investment causing a race to the bottom, see Ann-Sofie Isaksson and Andreas Kotsadam, “Racing to the bottom? Chinese development projects and trade union involvement in Africa,” World Development 106 (June 2018), https://doi.org/10.1016/j.worlddev.2018.02.003. For evidence of Southeast Asian nations racing to the bottom, see Ozay Mehmet and Akbar Tavakioli, “Does Foreign Direct Investment Cause a Race to the Bottom?”, Journal of the Asia Pacific Economy 8, no. 2 (2003), 133-156, DOI: 10.1080/1354786032000074712.


52. The FIFP is a relatively new initiative (it replaced the FIPB in May 2017), and thus there have been no formal evaluations of its efficiency relative to the FIPB. This is an area of potential future research. Regardless, the FIPB was established in order “to speed up the FBI inflow and increase the transparency in the FDI approvals…” Regardless of whether that precise model is successful, ASEAN states ought to take the broad goal to heart in creating an expedited process. See Hemant Singh, “What is FIPB and why is it replaced by the Foreign Investment Facilitation Portal (FIFP),” Jagran Josh, August 22, 2019, https://www.jagranjosh.com/general-knowledge/what-is-fipb-and-why-is-it-replaced-by-fifp-1566460443-1.


Op-Ed

Countering China’s Maritime Threat Will Require a Larger U.S. Submarine Force

By Pat Wiedorn

In recent decades, China has worked to develop the capability to exercise full military control over its near seas. During an invasion of Taiwan, this capability would be used to deny enemies the ability to deploy troops or ships to the area. To counter this threat the United States needs a larger number of smaller, mission-focused submarines.

Recently, the People’s Liberation Army (PLA) showcased weapons that are linchpins of this strategy, including hypersonic missiles purportedly capable of overcoming U.S. missile defenses to attack ships and land targets.¹ China has also been expanding its maritime capability by building aircraft carriers and improved ships.² Though some analysts doubt the current capabilities of the PLA’s weapon systems,³ the direction it intends to pursue is clear—and with China’s resources I have no doubt it will achieve its technological goals.

In the event of a large maritime war, the only platforms able to overcome China’s anti-access capabilities will be U.S. submarines.

U.S. Chief of Naval Operations Admiral Jonathan Greenert and People’s Liberation Army Navy Commander in Chief Admiral Wu Shengli return ashore following tours of a Type-39B submarine and Type 22 Houbei missile boat on Lushun Naval Base in 2014. Greenert’s visit came at the mutual request of U.S. and Chinese leadership to strengthen existing military relations between the two navies through additional military exercises, port visits and exchanges to advance maritime cooperative efforts in the Asia-Pacific. Photo by the U.S. Navy/Chief Mass Communication Specialist Peter D. Lawlor.
In the event of a large maritime war, the only platforms able to overcome China’s anti-access capabilities will be U.S. submarines. China will be able to immediately attack any detectable target, especially surface ships, with overwhelming barrages of missiles. American ships have robust anti-missile defense systems, but the easiest way to defeat a ship with ten anti-missile systems is to fire eleven missiles at it. Submarines, however, would be able to enter areas otherwise denied by Chinese missile systems. In 2010, a modern Republic of Korea ship, Cheonan, was torpedoed and sunk by a North Korean mini-sub while Cheonan was actively searching for submarines. The fact that a North Korean submarine was able to sink a South Korean ship undetected despite South Korea’s technological advantage demonstrates the inherent stealth capabilities of the submarine platform.

China has been proactive in countering the U.S. submarine threat. It is reportedly developing advanced submarine-detection satellites and deploying an underwater “great wall” of sensors. However, any sensor potentially capable of detecting a submarine is definitely capable of detecting a surface ship. Thus, a nuclear-powered submarine remains much less vulnerable to missile attacks. It is a truism in the submarine force that it takes a submarine to combat another submarine. China has not lost sight of this strategic point; it already has a force of seventy submarines and is building more.

A maritime war with China is therefore likely to become a submarine war. A submarine war, in turn, will be a deadly numbers game. During the fight against Japan in World War II, the U.S. submarine force saw the highest casualty rate of any service, losing upwards of 20 percent of the total ships deployed. I see no reason to assume a lower casualty rate during a war with China; the fundamentals of submarine warfare remain unchanged. A small fleet will be crippled after suffering casualty rates that high.

Unfortunately, since the end of the Cold War, U.S. submarines have become larger and more expensive. The current class of fast-attack submarines cost
$3.2 billion each, and the next class are expected to cost as much as $6 billion each. The expensive cost of each submarine has led to a decrease in fleet size. Over the next decade the U.S. submarine force will shrink to forty-two ships, its smallest size since World War II.

The United States cannot rely on the superiority of U.S. submarines to compensate for reduced numbers. Even if you optimistically assume U.S. submarines are twice as good as their Chinese counterparts, a Chinese fleet twice as large as the U.S. fleet returns China to tactical parity. And it will be a deadly mistake to assume a Chinese submarine with an experienced captain will only be half as good as a U.S. ship.

The solution, therefore, is to build more submarines. The Navy’s budget is unlikely to increase enough to fund more of the current classes of submarines. In a pair of articles for the Center for International Maritime Security, Duane Truitt instead describes a smaller and cheaper ship that would be ideal for a submarine-centered strategy to counter China.\(^{10}\) He compares his proposed ship to previous classes that cost $700 million each in 2019 dollars. These cost savings result from improved reactor designs and shedding land-attack missiles, leaving a submarine narrowly focused on sea control and attacks upon surface and subsurface units. These would, effectively, give more bang for the buck against enemy submarines.

If China invades Taiwan, its main priority will be to deny enemy units the ability to operate in its near seas. China will use missiles, surface units, and subsurface units to protect its supply lines between the mainland and Taiwan. The American response will be, in turn, to breach these defenses and destroy as many of China’s warships and shipping fleet as possible. This battle will see high casualties on both sides, and the only thing that will ensure the fleet’s survival will be the size of the fleet at the beginning of the war. Without an unlimited budget, the only effective way to increase the size of the submarine fleet will be to build a larger number of smaller, cheaper ships. This is a strategic imperative to ensure the United States can provide an effective check on Chinese aggression in the Western Pacific. ■
ABOUT THE AUTHOR

Pat Wiedorn graduated from the United States Naval Academy in 2011 with a B.S. in chemistry. After commissioning as a submarine officer, he qualified to operate naval nuclear reactors and then reported to the USS Oklahoma City (SSN-723), a fast-attack submarine then stationed in Guam. As a submarine officer, Pat lead sailors and conducted missions vital to national security in the western Pacific. After resigning his commission, Pat served as a Peace Corps Volunteer in Zambia. There, he taught fish farming and integrated farming techniques to rural farmers. At Yale, Pat focuses his studies on international development.

ENDNOTES


PHOTO ESSAY
OUTSOURCED LIVES IN SOUTH KOREA

By Tae Eom

On December 18, 2018, at Seoul’s Gwanghwamun Square, I encountered a drawing of a young Korean man whose eyes conveyed that he had many stories to tell. I realized it was part of a temporary memorial arranged for the young man, Kim Yong-gyun. I took out my phone to search for his name on the Internet.

Kim's name appeared on top of the trending news section, which featured articles from international news agencies. They detailed that one week prior, 24-year-old Kim, a subcontractor, was working a night shift alone at a thermal power plant when he was found dead at midnight. He appeared to have died after getting trapped under a conveyor belt, though his body was in a terrible state because the machinery could not immediately be shut down. When his family later searched his bag, they found a container of Cup Noodles and a broken flashlight.

Some distance from the memorial, a group of South Korean (sub)contractors, or “irregular workers,” congregated before news cameras to commemorate Kim's death and announce a massive rally against employment inequalities and discrimination scheduled for the following weekend. Spreading containers of Cup Noodles on the ground, they further bemoaned that the outsourcing of dangerous, dirty, and difficult projects led to Kim’s death. They cried, “We are all Kim Yong-gyun” and demanded an end to the “outsourcing of danger and death.” But how did this tragedy happen in the first place?

Following the 1997 Asian financial crisis, the number of contract workers in South Korea increased as Korean companies which had replaced lifelong jobs with temporary positions under the flag of flexible employment.

The statue of Admiral Yi Sun-shin stands at Gwanghwamun Square in Seoul, seemingly guarding the young Korean man in the picture. Because of its geographical proximity to the Blue House (the Korean President's office) and national government offices, sociopolitical issues in South Korea often flow into this open public space.
the companies began hiring young, unskilled contract workers on a temporary basis to further reduce costs—the companies did not even properly train them before letting them work alone like Kim’s case. As a result of the disappearance of lifetime employment, employment stability decreased, widening the gap between working classes, generations, and genders, and it deepened socioeconomic inequalities in terms of quality of life.⁵

In response to Kim’s death, the South Korean National Assembly passed a revised industrial safety bill, the Kim Yong-gyun Bill, at the end of 2018.⁶ In March 2019, Lee Sang-heon, the International Labor Organization’s (ILO) Employment Policy Department Director, visited Seoul. While commenting on Kim’s death, he recommended at South Korea ratify four of the ILO’s eight key conventions.⁷ The ratification of these conventions could make it possible for irregular workers, including laid-off workers, to organize and join a labor union and negotiate their labor environment with their employers, as well as not be forced to work.

The European Union has also been urging South Korea to pass such a bill as the ratification of the ILO’s key conventions was one of the South Korea-EU FTA provisions.⁸ Both South Korea and the EU agreed to establish an expert
panel that is currently investigating the South Korean government’s progress towards ratification. In addition, the United Nations’ Committee on Economic, Social, and Cultural Rights recently joined the EU in criticizing Seoul for insufficient legislative efforts. Some researchers warn that the international community will likely exert more pressure on the South Korean government with economic sanctions.

On August 19, 2019, eight months after Kim’s death and my time at Gwanghwamun Square, a special investigation committee concluded that Kim had followed all the rules, and the outsourcing of dangerous work without proper safety measures was the main cause of his death. The international community has become increasingly concerned with South Korea’s labor conditions and its failure to ratify the four remaining ILO conventions. Consequently, South Korean “irregular workers” remain vulnerable to low incomes, violence, danger, and even death.
태안화력 24세 하청노동자
故 김용균님의 명복을 빕니다.

죽음의 외주화를 중단하라, 직접고용 정규직 전환하라...
1년 넘게 외쳤던 발전소 비정규직 노동자들은
12월 11일 새벽, 또 한 명의 동료를 잃고 말았습니다.
ABOUT THE AUTHOR

Tae Yeon Eom is a Ph.D. candidate in Asian Studies at the University of British Columbia. His research covers a wide range of theories and case studies in international relations and diplomatic history. He is deeply interested in capturing contemporary and global socio-political issues with his camera and also likes to write articles for photojournals.

ENDNOTES


psychological stress of job insecurity impair irregular workers’ health more easily.


The Coming Catastrophe in Syria’s Prisons

By Karim Khalifeh and Karam Alhamad

As the novel coronavirus spreads across the world, health organizations are predicting a humanitarian catastrophe in war-torn Syria. In the absence of adequate health infrastructure, Syria’s political detainees—who are among the country’s most vulnerable population—face an impending humanitarian disaster. To avert this disaster, policymakers must push the Syrian regime to release these detainees immediately.

Nine years of nonstop war have left the Syrian medical system in ruins. In the country’s northeast, there are only ten adult ventilators for a region of two million people. In northwestern Syria, which has a population of four million—including one million who were internally displaced recently—there are only three fully-equipped hospitals. As a result, doctors estimate that over 100,000 people could die of the coronavirus disease (COVID-19) in the northwestern province of Idlib province alone.

While humanitarian organizations scramble to protect displaced Syrians living in refugee camps, few have voiced concern over Syria’s political prisoners who are languishing in Assad’s detention centers. Syria’s detention centers currently hold an estimated 128,000 detainees, many of whom are prisoners of conscience, political activists, human rights defenders, and peaceful protestors arbitrarily detained by the Assad regime. If the Syrian government does not release political prisoners immediately, they will once again have the blood of innocent lives on their hands.

Regularly subjected to torture, the prisoners will soon face something that may prove even more lethal: COVID-19. The squalid conditions in the re-

Two people walk down a bombed street in DeirEzzor, Syria in 2013. Seven years later, prisoners from DeirEzzor and the rest of Syria still sit in prison cells, subjected to torture and susceptible to diseases like COVID-19. Photo by Karam Alhamad.
gime’s detention centers are ideal for spreading coronavirus. Social distancing is impossible in the overcrowded prisons, which often keep up to 50 people in a single 4-by-6-meter cell. Prisoners have no access to clean water and cannot wash themselves or sanitize their cells. Furthermore, most detainees, already in poor health, have no access to medical care. These cold, dark, and damp prisons are likely to be epicenters of massive outbreaks of COVID-19. In Assad’s prisons, there are no hand sanitizers or surgical masks, no ventilators or intensive care units. In Assad’s prisons, if you get sick, you die.

Mohammad Badran, a former prisoner of the Military Intelligence’s notoriously horrific Branch 291 Center, knows first-hand the toll that a disease like COVID-19 could wreak on Syria’s prisons. He told us that detainees will not survive an outbreak of coronavirus— even a minor illness can spell death in a Syrian prison. Recalling the conditions of his cell, he lamented, “We were left to die. Many people who just got diarrhea died from it.” The inmates’ dead bodies were often left to rot for days in the overcrowded cell. He added, “If the coronavirus had entered the cell that I was in, not a single person would have survived, whether young or old.”

Some Syrians worry that Assad will purposely use the pandemic to rid himself of political problems. Samar Allouni, a refugee, joined her children in the Netherlands four weeks ago after fleeing Syria. However, her newfound safety is bittersweet. Her husband remains in a Syrian prison, where he has been since the Syrian regime threw him in a detention center on Christmas Eve almost six years ago. Samar hasn’t seen him since, and she isn’t even sure if he is still alive. Now she worries the regime is planning to use COVID-19 to get rid of detainees, including her husband.

“Who would stop Assad if he used [the virus] as another weapon for the mass killing of the political detainees? Don’t tell me he can’t.” Choking up, Samar reflected on COVID-19 lockdowns in European countries, observing that “people feel dead after being locked in for a few weeks, but my husband has been locked up for years now.” Even after almost six years, Samar still
hopes that her children will get to see their father alive again, but she is not counting on the international community to step in. She ended our interview despondently, saying, “Don’t bother telling the world’s governments to stop [Assad]. They’ve all failed us.”

Despite Samar’s cynicism, the international community should seize on this moment to push the Assad regime to release these prisoners. The Syrian conflict is finally starting to wind down, with the key parties involved in the conflict moving towards a political solution. Any eventual solution, as the UN Security Council unanimously declared when it adopted Resolution 2254 in 2015, must include the release of detainees. Though little progress has been made since 2015, recent shifts in the political landscape make a peace deal more likely today than ever before. For example, Moscow—one of the only players with enough leverage over the Syrian regime to advocate the release of detainees—recently signaled its strong desire to accelerate the peace process.

As the major players in Syria shift towards a political solution, a strategic window of opportunity to secure prisoner releases is opening. However, to ensure the moment isn’t wasted, the international community must immediately mount a pressure campaign. Russia has little incentive to push Assad without a concerted effort from the United States, European Union, and United Nations to demand the release of detainees. A release would not only avert a humanitarian catastrophe but could also serve as a confidence-building measure in the fragile peacemaking process. As Geir Pederson, the UN Special Envoy for Syria, noted in October 2019, a release of prisoners would “send a very powerful signal that we are indeed serious about making a new beginning for Syria.” Such a confidence-building gesture should be attractive to Russia, which seeks a political resolution to the conflict. Now, with a humanitarian catastrophe looming, the time is riper than ever to push the Assad regime to release the thousands of political prisoners that it is currently holding in its detention centers.

As of publication, there have only been nineteen COVID-19 cases and two deaths in Syria. But the reality on the ground is likely much worse. Some humanitarian organizations are already scaling back their presence on the ground and closing offices, and soon there might be no one left to help one of Syria’s most vulnerable populations. It is only a matter of time before Syria is overrun with the virus and its overburdened medical infrastructure collapses.
If the international community does nothing, thousands of political prisoners, activists, and dissidents in Syria’s prisons will almost certainly be among the first to die.

ABOUT THE AUTHORS

Karim Khalifeh graduated from Yale University in 2019 with an MA in Global Affairs. He was awarded the Fulbright Scholarship in 2017 and the Davis Fellowship for Peace in 2018. Currently, Karim works on advocacy campaigns for civilian protection in conflict areas, particularly in the MENA region. Before Yale, Karim worked at a Beirut-based bank.

Karam Alhamad is an international development professional, grants specialist, and policy advocate, with over 8 years of experience in project management, research, monitoring and evaluation, and 5 years of experience working with USAID/OTI, NEA/AC and DFID funded programs.

ENDNOTES


6. Mohammad Badran is a pseudonym. Mohammed, along with his family, remains in Syria, and he fears for his safety if his identity were to be revealed.


10. Author interview by phone, March 31, 2020.


A growing consensus among U.S. military leadership and policy makers is that offensive strategies have an advantage over defensive strategies in cyberspace. However, this consensus is based on a series of misperceptions. The first misperception is the inflation of cyber threats. The second is the misperception that both disruption and espionage strategies...
are the same as degradation strategies (deterioration in the operability of information systems). These misperceptions confuse the reality that the cost/benefit calculation of skills and expertise required in degradation operations favors the defense, not the offense. This article explains the logic behind these misperceptions and addresses how they influence assumptions indicating offensive advantages. Next, the article presents two mechanisms which demonstrate the advantages of defensive strategies. Lastly, the dangers associated with offensive biases and the emergence of a new “cult of the offensive” current cybersecurity strategy are discussed.

THE MISPERCEPTIONS OF OFFENSIVE ADVANTAGE

Cyber strategy suffers from two misperceptions: an inflation of threats and a conflation of strategies. In their book *Cyber Strategy: The Evolving Character of Power and Coercion*, Brandon Valeriano, the Donald Bren Chair of Armed Conflict at the Marine Corps University, and Benjamin Jensen, associate professor at Marine Corps University, categorize cyber strategies into three groups: espionage, disruption, and degradation strategies.

Espionage operations seek to obtain advantageous positioning through the theft or manipulation of information. The 2015 hack of the Office of Personnel Management (OPM), which compromised the security of 22 million U.S. citizens’ personal information, is an example of how the Chinese government stole the personal information of U.S. government employees and their contacts. Disruption operations are generally conducted to assess an adversary’s defenses and/or to limit or temporarily deny access to specific information or information systems, typically for propaganda purposes or for political statements. In 2007, Russian government and national hackers conducted a concerted Denial of Service (DDoS) campaign against Estonian government and banking information systems to protest the removal of a statue honoring Russian soldiers who died during World War II. Lastly, there is degradation, which has the objective of damaging an enemy’s networks, operations, or physical information systems. To date, the most notable degradation operation was the U.S. Stuxnet virus which the U.S. employed to target and destroy Iranian centrifuges. The misperception pertaining to the conflation of strategy is that espionage and disruption strategies are often considered to be the same as degradation.
Before delving into the misperceptions surrounding offensive advantage, it is necessary to define cyberspace in order to provide insight into the objectives of cyber strategies. Daniel Kuehl, professor of military strategy and national security policy at National Defense University, considers the defining characteristics of cyberspace to be the utilization of electronics and the electromagnetic spectrum to distribute, cache, manipulate, share, and exploit information through the use of mutually dependent and connected systems of communication devices. The objectives of cyber operations are information and information-based systems, as opposed to the traditional objectives of terrestrial-based warfare.

**Threat Inflation**

The first misperception that feeds incorrect assumptions of offensive advantage in cyber warfare, threat inflation, generates a fear of the destructive potential of cyberattacks. In 2012, Defense Secretary Leon Panetta warned that the United States faced the threat of suffering a “cyber-Pearl Harbor,” the effects of which could range from train derailments to power grids being shut down. While Panetta is correct in acknowledging vulnerabilities within infrastructure information systems that could be exploited, his comments echo a growing trend of inflating cyber threats beyond necessity and are problematic in several ways. First, the effects of degradation operations seek to mimic those of real-world effects. For example, a degradation operation targeting the U.S. electrical grid would produce similar effects to that of the 2003 blackout, which impacted a great portion of the northeastern U.S. and Canada. Despite nearly 50 million Americans being affected, power was restored within two days and no outage-related deaths occurred during this period. Additionally, although power was out, satellite imagery of the affected area shows that most affected areas—primarily large population centers—retained power via backup generators, therefore mitigating the impacts of the loss of power [See Figure 1]. Had this scenario been the result of a degradation operation, it fails to paint the catastrophic picture that Panetta’s Pearl Harbor comparison evokes.

As a result, the second problem is that Panetta’s warnings present a fallacy in establishing causal links between opportunity and outcome. In arguing that the existence of certain vulnerabilities could lead to a Pearl Harbor-like catastrophe, he is exaggerating the effects of degradation operations and blurring the lines
Figure 1: Satellite Imagery of the affected area just before and during the 2003 blackout. Note that major population centers still retained significant amounts of electrical power due to backup generators.
between what is possible versus what is actually feasible. Lastly, overstating cyber threats to this degree contributes to threat inflation. Exaggerating the effectiveness or severity of cyberattacks, even to increase awareness of vulnerabilities, distorts both the threat and the needed response. In the case of Panetta’s Pearl Harbor scenario, his exaggeration of the threat and the United States’ vulnerabilities obscures the reality that the only actors with sufficient resources to even possibly shutdown significant portions of the U.S. electrical grid are Russia or China and even then, neither possess the capabilities required to cause the level of physical destruction Panetta fears through cyber means alone.

To understand the real danger of cyber threats, it is necessary to begin with understanding what constitutes an act of force in cyberspace. When assessing what constitutes advantages for the offense in terrestrial warfare, Robert Jervis, the Adlai E. Stevenson Professor of International Politics at Columbia University, states that offensive advantage is determined when it is easier to destroy the enemy and occupy their territory than it is to defend against attack. The inverse is also true when determining defensive advantages. Although the objectives differ between the type of warfare Jervis refers to and warfare in cyberspace, the notion of force underpins offensive strategies. Determining an advantage between the offense and defense is measured by the relative ease with which force either destroys or can be defended against.

Nineteenth century Prussian general and military theorist, Carl von Clausewitz, observes force as central to warfare in his book *On War*, stating “war is thus an act of force to compel our enemy to do our will.” Clausewitz’s conception of force is physical and violent in nature. Thomas Rid, Professor of Strategic Studies at Johns Hopkins University’s School of Advanced International Studies, lists three criteria which he asserts constitute the essence of warfare and claims that no existing offensive cyber capability meets all three criteria. Going further, Rid states that, to date, only a small number of cyberattacks even meet one of the criteria. The question then is, if offensive strategies and capabilities in cyberspace are incapable of exerting force and do not meet the criteria for warfare in the cyber domain, then how are offensive actions and strategies in cyberspace classified? The answer is complicated. It is well-documented that most actions and strategies in cyberspace are incapable of generating any type of physical force by which adversaries can be compelled. However, degradation strategies and operations arguably pos-
sess the most destructive potential of all cyber strategies and come the closest to producing what resembles an act of physical force in cyberspace.

This analysis will focus exclusively on degradation when discussing cyberwarfare and the offense/defense balance. While espionage and disruption strategies are intertwined with degradation, they are given less weight in their impact on the offense/defense balance as their offensive potential is not capable of producing the same type of physical effects as degradation. In other words, not all cyber strategies are created equally.

Conflation of Strategies

Combinations with synergistic effects are important. Nearly all recorded instances of degradation have had correlating espionage activities associated with them.\textsuperscript{15} Espionage is required to infiltrate a network to degrade it by exploiting key vulnerabilities within the system. The reason these strategies are often conflated is because the general assumption, as Panetta demonstrates, is that the objectives of all cyber strategies are to degrade. While espionage and disruption often precede degradation, they have independent objectives that make them distinct from degradation. The danger in conflating espionage and disruption with degradation is that the conflation generates fear and misperceptions which can result in overreactions and aggression.

The primary objectives of espionage strategies are to infiltrate a network in order to monitor activity and steal or manipulate information. They are relatively easy as there are countless ways to covertly gain access to a network and steal information with little monetary expense. Disruption strategies seek to inhibit or prevent either individual or group access to a network, network function, or information. While disruption can be a more complex operation, depending on the objective, they are still relatively easy to conduct. For example, in the denial attacks against Estonia in 2007, lines of code and in-
Instructions on how to use them to conduct DDoS attacks were found in such innocuous places as forum pages. However, these strategies do not degrade networks or network systems to any lasting or physical degree.

Degrading a network is very costly in terms of time, money, and skills and expertise, explaining their infrequent use. Furthermore, degradation operations, contrary to what many believe, rarely result in either short- or long-term effects equal to the costs necessary to carry out an operation of this type. For example, Stuxnet, one of the most well-known degradation attacks in recent time, cost the United States an estimated $300 million dollars over a six-year period of research, development, and implementation. Despite becoming the foremost example of a degradation operation’s destructive potential, its success has been largely exaggerated. The Stuxnet virus only succeeded in shutting down 984 Iranian centrifuges, a mere 30% of Iran’s total production capacity, and only setback Iran’s enrichment timetable by one to two years. In addition, the International Atomic Energy Agency believes that Iran was able to supplement the loss of production by overworking its remaining centrifuges, resulting in overall positive enrichment production estimates. As this example demonstrates, despite degradation operations being the only type of cyber operation capable of manifesting physical effects, its destructive potential is often overstated. The danger in placing espionage and disruption in the same category as degradation is that it generates the perception that conducting operations in cyberspace that have the potential destructive capability of degradation are cheap, easy, and that nearly anyone can do it.

Of the 272 recorded cyber operations between opposing states from 2000 to 2016, only 40 (~14%) degraded or sabotaged networks or systems in any significant manner.

Of the 272 recorded cyber operations between opposing states from 2000 to 2016, only 40 (~14%) degraded or sabotaged networks or systems in any significant manner. Each of these 272 operations, were likely to have thousands, if not millions, of individual activities, none of which resulted in a
single casualty. In contrast to the reality of these numbers, seventy percent of Americans fear that the United States will suffer a devastating cyberattack that cripples critical infrastructure or destabilizes financial institutions. The side-by-side comparison of these figures highlights how conflation of strategies has generated a disproportionate amount of fear around the possibility of danger, which in reality is unlikely. Much of this problem relates to how we talk about cyberspace and what occurs within the domain. Harvard University International Relations Professor Stephen Wal, in addressing threat inflation, states, “putting the phrase ‘cyber’ in front of almost any noun makes it sound trendy and a bit more frightening.” He’s not wrong. The perception of offensive advantage has been unduly influenced by threat inflation and the conflation of espionage and disruption strategies with degradation. The following section will discuss the advantages defense has over offense, making it the dominant and preferable cyber strategy.

THE DEFENSE IN CYBERSPACE

The offense-defense balance plays an integral part in the stability or instability of the security dilemma. Determining an offensive or defensive advantage is one of two variables Jervis observes as influencing the balance. The objective of this section will be to apply the two mechanisms Jervis uses to ascertain an offensive or defensive advantage to demonstrate how the defense has the advantage in cyberspace.

Geography

Terrestrial borders and boundaries do not exist in the information domain, at least not in any manner that mirrors what we see when looking at a map or how Jervis conceptualizes geography and its importance as a contributing factor to the offense-defense balance. Most who have written on the offense-defense balance in cyberspace believe geography is a seemingly irrelevant measurement when determining offensive or defensive dominance. However, geography is an important factor in cyberspace and benefits the defense, a utility which many have been overlooked and dismissed.

While geography has value throughout all the levels of war, Jervis summarizes that anything which serves to increase the distance which an attacker must traverse, or makes the attacker vulnerable while traversing, subsequently in-
creases the advantage for the defense. Increasing time and distance is easily done by developing firewalls, encrypting data, utilizing air-gap networks, etc. However, these are passive defensive measures which usually only serve to delay a persistent attacker.

The benefit of geography within cyberspace is that it is synthetic. The defender is able to create the “ground” they fight on and can continually shape the “terrain” to their advantage.

The malleable geography of networks and information systems creates an inherent defensive advantage. Adopting an active and integrated defense within cyberspace, where networks and network components can continually be reconfigured and redesigned, significantly increases the cost of resources and time attackers would have to dedicate to find and exploit a breach.

Technology and Skills

The matter of technology is another mechanism that Jervis applies to determine an advantage between the offense and defense. Jervis states that the security dilemma is most dangerous when alliances, strategy, or technology dictate that security can only be assured through aggression and offensive action. The general consensus is that technology favors the offense. However, the matter of technology suffers from many of the same misperceptions listed above.
THE DIFFERENCE BETWEEN TECHNOLOGY, SKILLS, AND EXPERTISE

Some analysts infer that the nature of technology, its speed and ease of use, denote an offensive advantage.\textsuperscript{25} However, this is an incomplete assessment as it assumes these traits of technology are naturally occurring phenomena. The qualities listed and technology’s effectiveness are derived from the interaction between technology and human ingenuity. Cyber weapons, unlike conventional weapons, are inseparable from skills.\textsuperscript{26} The development and production of conventional weapons require a distinctive set of skills and expertise than those necessary to deploy them within a battlespace. Conversely, the skills and expertise required for developing and producing cyberweapons are the same used to employ them. In regards to cyberweapons, Alan Paller, founder of the Escal Institute of Advanced Technologies (SANS) claims the inverse to be true; “Skills are the weapon.”\textsuperscript{27} Paller is correct in noting that skills, more than the capabilities themselves, are what matter when discussing cyberweapons. Absent from skills, cyberweapons suffer from impermanence. In other words, most cyberweapons only work once. This makes skills and expertise, more than the technological capability, the unit of analysis when determining whether technology benefits the offense or defense.

A problem that emerges is that skills and expertise are neutral. They can influence the effectiveness of both the offense and the defense. A dependent variable when ascertaining an advantage between the offense and defense, in relation to skills, is cost. Do skills and expertise cost the offense or defense more? This question returns to the earlier distinction between the type of strategies and operations that can be employed in cyberspace. It is widely accepted that espionage and disruption strategies often employ cheaply conducted operations and as a result the balance of costs favors the offense. However, the effects that these operations produce, both in means of coercive force and more physical force, are severely limited, arguably negating their advantage to the offense. The strategy which does apply in accurately measuring the offense-defense balance is degradation.
SKILLS AND EXPERTISE APPLIED TO THE OFFENSE/DEFENSE DEBATE

The consensus is that the offense is heavily favored regarding degradation operations. This view stems from the perception that in order to be successful, the defense must counter all attacks, whereas the attacker merely needs to find a single entry point to exploit in order to be successful. While this perspective is technically correct in a broad sense, it suffers from the same conflation mentioned earlier. Espionage and disruption strategies dominate the offensive advantage perspective, creating pessimism surrounding the effectiveness of the defense. However, it must be reiterated that these strategies and operations are actually less impactful to the offense/defense balance debate due to their low-cost, low-payoff dividends. This misperception of offensive advantage attributes the cost efficiency of espionage and disruption operations to those of degradation as well. The reality is that the cost/benefit calculation of skills and expertise required in degradation operations actually favors the defense.

The cost/benefit and the requisite skills and expertise needed to carry out a degradation operation are nearly identical to those of the defense. Computer security expert Matthew Monte, observes this equilibrium in his book Network Attacks and Exploitation, stating, “Breaking into a particular network may be cheap after the tools and infrastructure are in place,” but “building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and training. This is not cheap.” Simply put, degradation strategies and operations require the same, if not more, skills, expertise, and money than it does to defend against them. This logic stands to reason that if the costs of the offense and defense are similar, then why is the security dilemma in cyberspace worsening? Robert Jervis observes that if the costs of the offense and defense are comparative then arms races are less likely to occur, making it
possible for states to provide for their own security without overtly threatening the security of other actors, lessening the severity of the security dilemma.\textsuperscript{30} The answer is that the absence of stabilization is due to a “cult of the offensive” which has developed amongst leading military leadership and policy makers around the world.

**THE CULT OF THE CYBER OFFENSIVE**

In examining the outbreak of World War I, Jack Snyder, international relations professor at Columbia University, observes a similar instance of the security dilemma worsening when it ought to have stabilized. Prior to World War I, defensive strategies and operations were heavily favored, and yet war still occurred in 1914. The roots of the cyber “cult of the offensive” are threat inflation and the conflation of strategy. Conversely, Snyder’s conclusion is that the “cult of the offensive” precipitating World War I was due to poor civilian-military relations.\textsuperscript{31} However, the similarities lie in that they both influence policy and affect state output. Preceding World War I, the General Staffs throughout Europe succumbed to an offensive bias preventing them from accurately assessing the offense/defense balance which resulted in the pursuit of recklessly offensive planning. As this section will demonstrate, although the antecedent conditions may not be identical, a new “cult of the offensive” is forming in cyberspace, manifesting in present-day policy directions put forth by military leadership.

Valeriano and Jensen assert that, until recently, activities within the cyber domain have primarily been related to ideological political conflict and coercive diplomacy.\textsuperscript{32} However, developing policy in the United States is seemingly changing the nature of action within the domain from covert espionage to militarized operations.\textsuperscript{33} As of 2018, United States Cyber Command (USCYBERCOM) released its vision of what its posture in cyberspace ought to be, which advocated for the United States to pursue a policy of “persistent action.”\textsuperscript{34} USCYBERCOM’s vision has the stated objective of improving “the security and stability of cyberspace,”\textsuperscript{35} which will be accomplished by “scaling to the magnitude of the threat, removing constraints on our speed and agility, and maneuvering to counter adversaries and enhance our national security.”\textsuperscript{36} USCYBERCOM’s vision for the United States’ cyber posture is troubling due to its seemingly blasé inference of preemptive action. A closer examination of USCYBERCOM’S vision shows the influence that many of the misperceptions addressed throughout this analysis have on its strategies. In addition,
USCYBERCOMS’s vision reflects some of the beliefs about the course of a war where the offense is dominant or perceived as dominant. USCYBERCOM’s equivocation of couching offensive preemptive action as integral to its defensive plans demonstrates its offensive bias, which is generally an antecedent condition for the development of a “cult of the offensive.”

CONCLUSION

In addressing the misperceptions surrounding offensive advantage, this analysis has sought to dispel the notion that offensive strategies are dominant in cyberspace. This analysis has also demonstrated how the geography of cyberspace and the requisite skills and expertise needed to operate in the cyberspace domain favor the defense. It has also been suggested that much of U.S. policy in cyberspace has been influenced by misperceptions resulting in a “cult of the offensive” that generates a bias for offensive strategies. The coming months and years are crucial in confronting and addressing the misperceptions which generate a “cult of the offensive.” If these misperceptions are allowed to persist in influencing policy, it increases the risk of moving warfare out of the cyber domain and into the physical world. Sometimes the best defense is simply a good defense.

ABOUT THE AUTHOR

Charles Smythe is an MA candidate at Georgetown University’s School of Foreign Service. He is a decorated United States Marine Corps combat veteran of Operation Enduring Freedom where he served as an infantry vehicle commander. His research and academic interests focus on the regional security of the Korean Peninsula and security issues affecting regional stability.

ENDNOTES


12. Rid lists the criteria for force: the action must be violent, instrumental, and political.


33. Ibid.


35. Ibid.

36. Ibid., 2.

37. Jervis lists a series of beliefs of which two apply here, the first being that “war will be profitable for the winner” and the second that “wars are expected to be both frequent and short.” (Jervis 189). In cyberspace, the first belief is found in the perception that espionage and disruption strategies are profitable as they are both cheap. The second belief stems from the fact that most conflict in cyberspace is measured in mere seconds or shorter spans of time.
INTERVIEW

“AT ALL COSTS”

Former U.N. Syria Envoy Staffan de Mistura Recounts Unrelenting Efforts Towards Peace

By Matt Trevithick

Staffan de Mistura, an Italian-Swedish diplomat with a 40-year career in the United Nations, last served as the UN Special Envoy for Syria from 2014 to 2018. Appointed by UN Secretary-General Ban Ki-moon in 2014, he worked tirelessly with all sides in the conflict to work towards peace, brokering ceasefires and reducing human suffering wherever possible. Executive Editor Matt Trevithick of the Yale Journal of International Affairs sat down with him shortly after President Trump’s announcement of a withdrawal of U.S. forces from Syria in October 2019.

Matt Trevithick (MT): Starting with your background and a bit about who you are, can you explain the process by which you came to be so involved in conflict zones and international humanitarian work?

Staffan de Mistura (SM): I wanted to be a fireman when I was a kid, and then I wanted to be a medical doctor. But then my father rightly reminded me that since I spoke five languages, why couldn’t I do something more international? I ended up in the job of being a de facto doctor of countries, seeing them as critical patients.

The critical point was when I volunteered in Cyprus when I was about 18, accompanying a World Food Programme food assessment mission. While I was working on the Green Line separating Turks and Greeks, I was exposed to something that changed my life: a child shot by a sniper. I was profoundly outraged because I could not understand why a kid who was playing football on the Green Line had to become a tool of showing who is stronger, when men did not have the courage to fight each other. That’s what should have

A young boy at the Za’atari Refugee Camp in Jordan, where nearly 80,000 Syrian refugees are living. Photo by the United Nations/Sahem Rababah.
been done instead of sniping at children. That level of outrage kept me going and is why I have been accepting jobs mainly in war zones – 21 missions in war zones over 47 years of service – always fueled by that level of outrage, by that one event.

**MT:** When you accepted the mission as the UN Special Envoy to Syria, what were you and the UN thinking about regarding the conflict, what were you preparing for, and what was in the works?

**SM:** I accepted the position in 2014. At the time, the UN was in a moment of great doubt, because the two preceding UN Special Envoys to Syria, Secretary General Kofi Annan and Lakhdar Brahimi, had given up. They decided to resign, the first after 8 months and the second after 14 months. The general conclusion was: Syria is “mission impossible” because there was very little space for a mediator, as the sides did not want to recognize each other. So, why did I accept? Many advised me not to take the position.

The UN at that time was in a vacuum. Brahimi left after the second major UN conference in Geneva failed. When the Secretary General called me in the middle of the night, I said well, it’s been 43 years of this, and I think it’s time for me to deliver someone else to this. But he sent me the statistics, and I saw how many people were being killed and slaughtered in this phase, which had not yet reached the 450,000 of today. I couldn’t sleep that night.

**MT:** What was that approach?

**SM:** From the lessons of my predecessors, you cannot and should not call a peace conference. Even if you think you have some changes. Why? Because
spoilers will spoil it. By doing so, you put all your eggs in that basket, and you put your identity and perhaps your ego into it as well. Then you have no other option then to say “I have to resign.” I devised a new technique I called geometry invariable. You never really call a conference. You invite sides for talks. You invite them for consultations. If they don’t agree in coming, you say, no problem, I’ll meet the others, and you can come when you’re ready, the door is always open. You don’t provide – as much as I could over four years – the occasion for any spoiler to play the final card.

There were no angels in this conflict, as you know well. In the beginning it appeared that one could make a distinction, but more and more it became difficult. Although some side did commit horrors, like the Syrian Government bombing the hell out of cities.

MT: There is a lot of gray area in war zones, but bombing hospitals seems like a very clear line.

SM: Bombing them twice!

MT: How did you respond to that? Was there anything you could do?

SM: There are many ways we tried to respond, but the moral response was: this is horrible. This was a complete breach of what used to be the rules of the game. Of course, when you listen to one side, they will say, “in that hospital they were keeping weapons. Behind it, they were hiding with rockets.” Whatever the reason. But you don’t hit the hospital, and you don’t hit it a second time to target the first responders.

Sadly, in this period of history, that taboo seems to have been broken. Why? Why on earth? Many actors felt remorse about this, but they told me the strategy – which is brutal – is very effective. The civilians, in particular those who have children, would like to think that, in spite of all the difficulties in a war zone, there is still a chance, in case my son is hurt, to bring him somewhere. But if that hope is gone, and my wife is pregnant, I better move. The whole idea was – by bombing the hospitals – you make civilians move, which means that the only ones left are the fighters. Therefore, you can bomb the hell out of it without being criticized for killing civilians. But in order to do so, you are actually killing civilians, so it is a horrible tactic.
We tried at a certain point by saying to the Syrian government and their allies – we will tell you where the hospitals are. We will put them on the map so there is no confusion. Because every time they tell us “there was a mistake” or “there was a misunderstanding.” We actually put a UN flag on the map locations of the hospitals, so they had a comprehensive list. Then, if they hit them, they cannot claim a mistake. Believe it or not, even that was not enough. Eventually even those hospitals said “we don’t want to be marked.”

**MT:** What does it take to work together with the Syrian Government on a day-to-day basis in Damascus? What does that relationship look like?

**SM:** During my time, I had no option but to be extremely critical and try to interfere wherever I could to what I saw as a brutal, medieval siege. Eastern Ghouta, Darayya, Aleppo, and so on. With barrel bombs being dropped all over the country, all over dense civil areas. Inaccurate and brutal.

My approach was to meet them and tell them, “I can’t imagine that you believe that even if you win the war, you think you can go back to normality by doing this.” Why can’t we find some formula by which you avoid bombing a whole city because in one area you have terrorists. You don’t destroy all of Manhattan because one street is full of problems. Their answer was always defiant. But that doesn’t mean I shouldn’t be defiant too.

First, the reason I left was deeply personal. It was clear the war – and I insist on that word, the war – had been almost won territorially by Bashar al-Assad thanks to the support he got from Russia and Iran. No doubt about it. You need to not only win the territory, but you need to win the peace as well. That’s the real challenge.

My successor didn’t see – with his eyes – the bombing. So, like a doctor, he only picked up the patient from where it was. That’s what he’s trying to do. But I still had some doubts at the end of my tenure. Perhaps I could do the last push at the end of the war.
A group of analysts who had been studying war all over the world contacted me. They said, Mr. de Mistura, you may be having some doubts about your departure. But you should know that these days, hardly any war ends with a conference. There is no Treaty of Versailles or Dayton Accords. You have a meeting, acknowledging the deflection, defusal of the fighting; you find local arrangement, and you try to package it in some type of form that looks sustainable. And hopefully stays sustainable.

What you should know, they told me, is that during your four years, every month coming up with new ideas, a new convoy, meetings that were not productive but kept people talking – during that time the fighting was getting more and more embarrassing. By getting the Americans and the Russians to discuss a ceasefire, and by making public appeals and initiatives related to all this, we calculated that instead of 450,000 people killed, it would have been very close to 700,000. So that is what you and the UN should be feeling, even though you did not stop the war.

Remember, I wanted to be a doctor. Doctors can’t cure all diseases. Cancer, Alzheimer’s – you just can’t. Would you then resign, because you can’t cure one of these? Or would you rather, as most doctors in fact do, keep the patient alive, keep up the atmosphere of hope, and continue reducing pain? Tomorrow you may have a new entry point or new treatment.

This could be the moment we are seeing in Northern Syria today. When the United States made decisions to draw down, others are ending up winning the war and inheriting responsibility for the country. How do they make it more inclusive? How do they manage it responsibly? How do they avoid a new al-Qaeda? Maybe that will lead to some concessions, which may lead to a sustainable peace.

MT: What were the greatest UN successes in Syria?

SM: I would never call it a success because it’s like a punching bag. There were moments of breakthrough, but when I look back, there were one or two magic moments. First, when Russia and the United States came with a common approach, the other players did adjust. U.S. Secretary of State John Kerry and Russian Foreign Minister Sergey Lavrov met and came up with this Vienna Process, which I and the UN sponsored and supported. 27 countries,
including Iran and Saudi Arabia, sat at the same table in order to at least have some humanitarian aid convoys or some ceasefires.

Second, there was a magic moment when Kerry and Lavrov actually, with strong support from my side, came up with a very good agreement. In August 2017, the Russians agreed to guarantee grounding the Syrian Air Force. No helicopters. No airplanes. No Barrel Bombs. Most of the war for the government – most of the killing and destruction – had been fought from the air. Not very many ground battles. The United States were committing themselves to disconnect al-Nusra, which is a franchise of al-Qaeda by the way, from the rest of the Syrian opposition forces. That made sense. Only the United States and Russia would be the ones flying, with both aiming at al-Nusra, which should be the common enemy. Then the UN would be able to reach everywhere with convoys. If that would have been applied properly, we would have cut short the war.

But, spoilers jumped in and ruined the chance, and we went back into the Battle of Aleppo. There were moments of light and hope, but then they quickly collapsed.

**MT:** Is there one moment that you remember particularly vividly from Damascus in your time there that will always be with you?

**SM:** I went though many moments where I asked, “What on earth are we doing here? Are we just witnessing a horror, or are we able to make a difference?” When it’s clear that the government wants to win the war, the opposition wants to win the war, and neither wants to negotiate.

Outside of Damascus, I met a woman with eight children, living in a tent. Her husband had been killed in a bombing, but he had nothing to do with the government or the opposition. He was one of the classic, typical victims
in Syria. When I came up with a ceasefire during the Vienna Process period, she told me, “I believe in the future of my country. And I will take this tent with my children, and bring them back to the place where my home has been destroyed by a bomb, because I will put a tent there. Because I want to believe in the future of my country.” This helped me a lot.

I saw this a lot in the Balkans, too. When you see people, particularly women, believing they can make a difference by insisting and hoping for their own country, we cannot abandon them.

**MT**: Is it important to keep the discussion going at all costs? Critics of the UN would suggest that talks for talks’ sake can’t be that important.

**SM**: Yes. At all costs. Because you may have new opportunities and new entry points to make change. That doesn’t mean you just talk. You have to make convoys, run vaccination campaigns, and still force those convoys through. There would have been many more victims if we had not done that. Talks are not important just for talks’ sake. Taken alone, talks could be a cover for continuing the war, which was never my intention.

**MT**: Do you think the fundamentals of the UN are sound? Or do we need to re-think some assumptions about how organizations like the UN respond to crises like Syria? Was Syria particularly bad and therefore an outlier, or are discussions on major policy shifts necessary?

---

**We learned about the Peace of Westphalia.**

**We need a Westphalia for the Middle East.**

---

**SM**: After 47 years in the UN, service with 9 UN agencies, and working with 4 Secretary Generals I think I can give a good perspective on this. There is a need of substantial re-thinking. There is a need for making sure that the UN response is much more preventive. The problem is that in order to be preventive, you need active cooperation between the Security Council, Secretary General, UN Secretariat, and member countries. It needs to be much more cohesive, thorough, and much more effective, no doubt. This requires a Security Council
that at least doesn’t stop this work through a veto. This has been a major tragedy, the use of vetoes when there is a humanitarian or human rights issue.

MT: What do you think the UN or the world has learned from the Syria Crisis?

SM: History will judge based on the outcome. The final outcome is what matters. But I think they learned that when there is a crisis, it needs to be addressed at the earliest stages.

There were three circles in the Syrian Conflict. The first circle was internal protests, mostly peaceful. The second circle became the regional involvement. On the one side, Saudi Arabia and its allies, and on the other, Iran. And then the third circle: Russia and the United States, playing a big power game in that environment. If you diagnose the disease early, you can make a major impact.

Secondly, there is an aspect which we have to recognize. The major reason for this type of crisis is a huge competition. Not only in Syria, but in Yemen, Lebanon, and Iraq between the Sunni and the Shia. Between Saudi Arabia and Iran. And we are being pulled into it. In Europe, we went through a long war between Catholics and Protestants. More recently, in the Balkans, between Orthodox Christians and the Muslims. We learned about the Peace of Westphalia. We need a Westphalia for the Middle East.

ABOUT THE AUTHOR

Matt Trevithick, a graduate student at Yale University, is a native of Boston, MA with a decade of experience on the ground in the Middle East and Central Asia in higher education and international development. He is a graduate of Boston University and recipient of their Distinguished Young Alumni Award. A member of the Dartmouth Conference—the longest continuous bilateral discussion between citizens of Russia and the United States to avoid nuclear war and strengthen ties—he also has a certificate in Persian language from Tehran University and has published widely in the American media on foreign policy issues.
OP-ED

BIT BY BYTE

Rebooting America’s Colombia Policy

By Eliot Pence

Colombia is at a critical turning point. Nearly two years after President Duque took power, the country now faces a refugee crisis now bigger than Syria’s, an exploding coca production problem, and the return of policy by protest. New technologies like computer vision, artificial intelligence, and autonomy are becoming more common and commercially available, dramatically reducing the cost of managing hard problems like border management, illicit drug production, and wide area surveillance. As the United States evaluates its partnership with Colombia, it would do well to revisit how it leverages technology to advance mutual interests.

President Duque hit the ground running two years ago when he became president. His charisma and knowledge of Washington and the “multilateral world” gave him a head start, to be sure, but his efforts have borne real fruit: Foreign Direct Investment has risen substantially—more than any other Latin American country. An accord with the Revolutionary Armed Forces of Colombia (FARC), an armed guerilla group, has been largely stable, if increasingly tenuous. Entrepreneurship and the tech industry—pillars of President Duque’s “Economía Naranja”—are now material contributors to growth and domestic demand.¹

As the United States evaluates its partnership with Colombia, it would do well to revisit how it leverages technology to advance mutual interests.

Ground teams manually destroying coca crops in Colombia. Photo by the U.S. Government Accountability Office.
But the accomplishments stand on uneven ground. As *Foreign Policy* notes, the number of Venezuelan refugees is set to surpass the number who have fled Syria—although they have received only 1.5 percent as much international aid.2 Venezuela’s disintegration has put acute pressure on the social and governing system President Duque has sought to build, giving oxygen to the National Liberation Army (ELN), an armed leftist group, and criminal traffickers. A thriving coca development industry also adds to Duque’s problems. According to a UN report, Colombia has more land producing coca than ever in its history. Land used to grow coca constitutes an area the size of Los Angeles—and it continues to increase by roughly 20 percent annually.3

After fifteen years and $10 billion in counter-narcotic assistance, recent American efforts to assist the Colombians have achieved mixed results. The core of U.S. strategy has been a stop-start transition from countering narcotics in “Plan Colombia,” the plan originally conceived of by the Pastrana/Clinton Administrations, to a partnership more focused on peace, reconciliation, and stabilization in “Peace Colombia.”4 These efforts would likely be more successful if the United States incorporated new technological advancements into its strategy in Colombia.

---

**A better approach would be to support the development and dissemination of new technologies and to combine them with rapidly commodified old technologies.**

---

The recent transfer of sixty helicopters to assist the Colombians in stemming the expansion of coca production is a case in point of the inefficiency of the current U.S. approach.5 In addition to having huge lifetime costs for partner countries, helicopters are an imperfect tool for surveillance and reconnaissance. A better approach would be to support the development and dissemination of new technologies and to combine them with rapidly commodified old technologies, like radar and other means of light detection, for Colombian front-line fighters.

Recent advances in machine learning and satellite imagery make tracking crop production much easier by picking up signatures of crop patterns and chem-
ical compounds from satellites. With advancements in lower orbit satellites, buying near real-time imagery can cost less than $10 for specified locations. Managing vast borders or interdicting smugglers is not a human-scale problem. Autonomous drones interlinked with smart, computer vision-enhanced ground sensors can better detect, classify, and coordinate response times to make manned missions effective, efficient, and safer. The lifetime cost of a sophisticated autonomous drone can be up to ten times less than a manned helicopter. Many of these technologies are being used by American security forces already.

American support for the ethical dissemination of next generation technology is increasingly urgent as Chinese companies seek to set global rules on the use of artificial intelligence in facial recognition. News this month that Chinese companies, Dahua and ZTE, are hoping to gain an edge in emerging markets, such as Colombia, by laying the groundwork for AI standards is especially concerning since Chinese investment in Colombia exploded in 2019. This November, Colombia signed a $4 billion deal with Chinese entities and announced its intention to join China’s Belt and Road infrastructure initiative, which it had previously resisted. Deploying new surveillance technologies in democratic societies is always fraught with ethical and governance considerations, but if the United States doesn’t take the lead in deploying these technologies, geopolitical rivals will, weakening US competitiveness and influence.

In a Congressional hearing earlier this year, Admiral Craig Faller regretted the gaps that U.S. forces have in intelligence surveillance and reconnaissance (ISR) for counter-narcotics: “We mitigate those gaps with different sources of intelligence...[but] we are deficient in our ISR for the counter-narcotics mission....[and] record cocaine [production in Colombia] is going to mean record drug flows.” Ultimately, better ISR enables U.S. partner forces to do more, and allows the United States to spend less. Whatever the next phase of America’s relationship with Colombia looks like, it is unlikely to look the same as the past fifteen years. Rather than focusing on the size of the assistance, policy makers should carefully examine what to fund in the first place.
ABOUT THE AUTHOR

Eliot Pence leads international expansion at Anduril Industries, an artificial intelligence and robotics startup. Prior to joining Anduril, Eliot founded and led McLarty Associates’ Africa practice from 2013-2018, where he remains a senior advisor, and co-founded Insider, Union House, and Tofino Capital. Eliot is a mentor at the Tsai Center for Innovative Thinking at Yale University, a member of the U.S. Trade Representative’s Trade Advisory Committee on Africa, and a term member of the Council on Foreign Relations. He received his M.A. from Yale University and B.A. from the University of Victoria.

ENDNOTES


A Social (Media) Contract
Reconciling American Freedom and Security in an Age of Online Radicalization and Extremism

By Tony Formica

INTRODUCTION: ONCE UPON A TIME IN AMERICA

2018 was proclaimed the most violent year for deaths caused by domestic extremists since the 1995 Oklahoma City Bombing, closing out with eleven Americans murdered in the Tree of Life Synagogue massacre.1 Extremist groups have been on the rise for the past four years, and an uptick in extremist-related violence has followed in their wake.2 Prominent social media platforms have been tacitly implicated in these attacks, facilitating extremist recruitment, disseminating propaganda, and spreading disinformation.

Neither leaders in our nation’s capital nor Silicon Valley have proposed meaningful solutions to address this threat. Should Congress regulate tech firms? Criminalize certain types of online behavior? Trust in private sector self-regulation? These questions reveal an underlying tension between sacrosanct American public liberties, venerated corporate rights, and the desire of American citizens to be secure in their daily lives.

Censorship and surveillance will not solve this dilemma; they seem likely to exacerbate it. We need a paradigmatic shift in how we view the intersection of online extremism with protected liberties and corporate rights. Domestic extremism is an unquestionable threat to national security, but the best way to deal with it lies in framing it as a public health issue and encouraging and reinforcing industry-led self-regulation. This approach optimally synchronizes tech sector know-how with governmental oversight practices in a manner that promotes public safety without abandoning our nation’s bedrock principles.

Social media platforms such as Twitter face enormous challenges fighting extremist recruitment, propaganda, and disinformation on their sites. Photo by Sara Kurfeß.
ADMIT IT, AMERICA: YOU HAVE A PROBLEM

Congress is dedicating an increasing share of its attention to the relationship between social media platforms and online extremism. Several hearings since 2017 suggest that Congressional focus on extremism is also shifting from traditional concerns (such as the recruitment of Americans to jihadist movements) to the blossoming threat of domestic extremist violence and proliferation of hate groups in the United States. Representative Jerrold Nadler convened a hearing in 2019 to examine whether social media firms’ efforts are sufficiently tackling hate speech and extremism on their platforms that are resulting in real-world deaths. As Representative Cedric Richmond put it: “There are real families being destroyed; there are real people dying because of this.”

The data supports these warnings: Islamic terrorism is quantitatively and qualitatively a lesser threat to American domestic tranquility and security than home-grown radicalized extremists. Domestic extremists accounted for nearly 74 percent of all extremist-related fatalities within the United States over the past decade, while Islamic terrorism claims slightly more than 23 percent. Domestic extremists would have a monopoly on fatal violence had not one of the perpetrators “switched from white supremacist to radical Islamist beliefs prior to committing [his] murder.” As their overall share of the violence increases, domestic extremists are also killing more Americans year-on-year. There was a 35 percent increase in the number of Americans killed by such groups from 2017 to 2018. This violence was accompanied by a surge in hate groups, hate group recruitment, and hate crimes, which have run unchecked since 2015. Right-wing extremist groups, in particular, are responsible for the majority of fatal domestic violence, presenting both hate group ideologies and extremist violence tendencies.
By comparison, since after September 11, 2001, through to 2018, Muslim Americans killed 141 of their fellow citizens; non-Islamic extremists killed 49 Americans in 2018 alone. There has been an overall downward trend in arrests of Muslim Americans for alleged involvement with violent extremism since 2015. This information suggests that narratives and radicalization pathways from overseas are less effective than homegrown varieties at enticing Americans to extremist violence.

These trends are driven at least in part by political polarization, anti-immigrant sentiment, and technologies such as social media, which help spread propaganda. Interestingly, today’s extremists prefer to operate as lone actors, employing firearms and bladed weapons. This is in stark contrast to bombings or arson, which predominated extremist violence in the United States throughout the 1990s and early 2000s. Today’s radicalized individuals have a clear preference for violence that is up close and personal.

What these observations do not provide is an understanding of the mechanisms which allow online antipathies to metastasize into real-world violence. Is there a causal link between violent behavior online and the demonstrated preference for intimate, close-range violence by domestic extremists? Social media’s distortion of our conceptions of physical space is at the core of understanding this connection.

A PATHOLOGY OF VIRTUAL HATRED AND REAL VIOLENCE

Social media disrupts conceptions of the physical and emotional distances between its users. An individual might feel tremendous affinity for someone in their Star Trek fan blog, perhaps feeling more affinity for his digital compatriot than for his next-door neighbor. Indeed, an individual might earnestly despise their neighbor, but there are social consequences for giving those feelings full expression. For example, screaming about your neighbor’s car parking might entice your neighbor to scratch up your car with his keys the next morning. However, no such inhibitions exist online because we are unlikely to encounter our online counterparts physically. The low risk of reciprocation produces no consequences for employing vitriolic or violent language against others online. In all of these cases, our conception of physical proximity in the digital world distorts the emotional attachments we develop with our online acquaintances.
These dynamics are not novel and underlie every modality of digital interaction. However, they interact with human cognition in dangerous and powerful ways when an individual is vulnerable to radicalization. Individuals, both on and offline, tend to seek out, share, and recall information that is compatible with their worldview and cultural commitments. Individuals search for information as motivated consumers, rather than as passive aggregators. People do not generally become extremists by happenstance online encounters. Instead, extremist-prone individuals tend to have affinities and worldviews, which lead them to actively search for online content that reinforce their beliefs. These preferences may be sourced as disinformation, misinformation, or extremist propaganda.

Social media algorithms note and log these extremism-prone search preferences, and subsequently steer users towards more of the same. This mechanism comprises the entire social media business model: algorithms learn about user preferences and steer them into communities of similar individuals with similar consumption patterns and preferences, and who collectively generates more clicks and revenue. A primary consequence of this process is the reduction of information-sharing across tribal units, including and especially in the case of extremist groups. The result is a communications environment where an individual’s information diet is restricted almost exclusively to the biases and preferences of people to whom they have been algorithmically guided.

Insular cultural nodes produced by this filtering effect are hard to break. While it is not impossible to acquire a diverse range of perspectives online, social media algorithms are programmed to keep users anchored to profit-maximizing communities. Human psychology amplifies the problem. Once an individual has a tribal allegiance, he tends to apply cultural cognition to reconcile any dissonance between his emotional commitments and perception of facts. Any countervailing information which breaks through the filters is discredited and discounted in the pursuit of ideological coherence at the expense of civic cohesion.

While these effects are amplified for extremist-prone individuals, even those less at-risk have a demonstrated tendency to abandon their inhibitions against uncivil rhetoric when engaging perceived adversaries online. The paucity of information from outside groups, paired with the recurrent discrediting of
any such information that does enter the tribe’s media feed, results in the dehumanization of external “others.”23 Viciousness against the tribe’s perceived enemies quickly becomes confused with virtuous defense of the tribe’s values. The dynamic reinforces when rival Tribe B punches back at Tribe A, confirming Tribe A’s suspicion that Tribe B’s members are irrational, ignorant, and, after enough iterations, malfeasant.24 Cognitive dissonance resolution mechanisms will persuade Tribe A’s members that their original savaging of Tribe B was not only justified, but also insufficient: Tribe B remains ignorant and irrational, thus meriting further abuse.25 The result is a digital commons of shouting parties and individuals, locked in perpetual digital combat, where neither side can agree on basic facts nor perceive each other as well-intentioned fellow citizens.

These interactions significantly increase the emotional distance between warring individuals online, increasing the probability that opponents eventually come to see their rivals as less human. That becomes more likely when an individual is entrenched in an online extremist group—such as a white nationalist movement—that specifically categorizes other groups as enemies or sub-humans. The distortion of physical proximity wrought by digital communications—individuals rarely, if ever, see their rivals in the real world—makes this perception tenable. The radicalization of emotional commitments and concomitant animosities makes it dangerous. Emotional and physical distance between killer and target are two of the most potent natural inhibitions human beings have against killing members of our own species.26 Military formations, for example, undertake significant desensitization efforts to cause their own soldiers to view the enemy as less than human.27 Unfortunately, social media can serve the same function for online warring tribes.

It is, therefore, no wonder that extremist and hate groups, and the crimes associated with them, have been on the rise: social media allows them to spread their message and guarantees people sympathetic to that message will find it. A percentage of these individuals will become sufficiently radicalized through

---

Social media allows them to spread their message and guarantees people sympathetic to that message will find it.
escalating intertribal conflict to become convinced that their enemies are malfeasant subhumans deserving of violence, and a smaller percentage will be motivated to translate their online conflict into acts of physical violence in the real world.

THE IMBROGLIO OF PUBLIC-PRIVATE ROLES AND RESPONSIBILITIES

The psychological pathology analysis above suggests two remedies for the threat posed by online radicalization and extremism. The first entails disrupting the radicalization process at its inception, via some form of intervention when a consumer searches for content linked to extremist perspectives, thus curbing the forces driving individuals into extremist enclaves. The second remedy entails platform operators employing a process that would allow them to identify, adjudicate, and remove extremist content on their sites, thus reducing the ability of motivated consumers to find harmful content catering to extremist preferences.

Unfortunately, sensationalism and division on social media platforms sell: no emotion goes viral faster than rage, and furious netizens are consistent platform users.27

Social media firms are concerned with promoting their bottom line and expanding their consumer base. These interests may conflict with a responsibility to promote public security. This responsibility lies with the government.

However, traditional government tools to combat online extremism—Foreign Intelligence Surveillance Act (FISA)-derived measures, Executive Order 12333 and related orders—have significant operational shortcomings.28 First, they are slow and outdated. Radicalization on social media platforms occurs faster than federal law enforcement agencies are capable of legally monitoring. Simply getting a FISA request approved to initiate Federal Bureau of Investigation (FBI) surveillance requires extensive evidence from multiple types of sources, vetting through several layers of organizational hierarchy and typically several rounds of editing between the Bureau and the Department of Justice (DOJ).29 Critically, a FISA warrant cannot “…be opened ‘solely on the basis of First Amendment activities,’” precluding the monitoring of American
citizens simply because they visit or associate with unsavory individuals, either on or offline.\textsuperscript{30}

Fundamentally, traditional government tools for surveilling extremism assume that Americans worthy of monitoring are working with or being manipulated by a hostile foreign actor; they offer little guidance on how to proceed when great numbers of Americans are being radicalized by their fellow countrymen. The greatest difficulty of government surveillance tools in the context of home-grown extremism is the threat these tools pose to the protected liberties of American citizens and their trust in government.\textsuperscript{31} These liberties do not simply concern the private citizen either. America’s commitment to free speech in the public forum is at the heart of our understanding of the public discourse required for effective democratic governance.\textsuperscript{32} Government-mandated social media censorship, whether it be removing content or blocking users, would represent a betrayal of First Amendment principles. Social media firms would justifiably see such restrictive regulatory approaches not only as threats to liberties, but also to profits, and in any event would deploy their legions of corporate lobbyists.

The current impasse in dealing with social media-derived domestic extremism stems from an outdated conception of government’s roles and responsibilities where national security clashes with private liberties. Furthermore, social media firms are critical to the implementation of any feasible policy solution. Frankly, social media firms possess the technical capabilities and capacity to expeditiously implement meaningful changes on their platforms. These firms must be integrated into any usable framework and that framework must entail more than simply a threatening ultimatum from Congress.

A more fruitful approach could entail observing past government approaches to regulating products inimical to public interest. Domestic online extremism
is a national security issue, but the most effective mitigation strategy does not lie within national defense or intelligence. It lies in industrial self-regulation.

RECOMMENDATIONS: DIGITAL DUTIES AND OBLIGATIONS

Industries often adopt voluntary self-regulatory procedures when they receive pressure from both lawmakers and the public.33 This has been observed in industries spanning from tobacco to marine fisheries.34 Social media firms currently face this dilemma. While effectiveness and earnestness of self-regulation will vary by industry, a rigorous self-regulatory framework is key: successful frameworks emphasize transparency, benchmarks, oversight, and accountability.35

Industries often adopt voluntary self-regulatory procedures when they receive pressure from both lawmakers and the public.

In the case of self-regulation, transparency refers to standards which are created by expert organizations external to the industry with widespread understanding and acceptance of these standards.36 Benchmarks are quantifiable measures of both performance and effectiveness; for example, the number of extremists detected on the platform, or the efficacy of content removal tools.37 Oversight demands regular reporting, and allows regulatory authorities to examine progress against defined benchmarks periodically.38 Finally, accountability mandates reports be available to the broader public with a mechanism for external parties to register dissatisfaction with self-regulatory procedures.39

Two major social media firms have implicitly recognized that self-regulation in response to online extremism and radicalization on their platforms is favorable. Facebook launched its Community Standards, which establishes guidelines governing violent, objectionable, and inauthentic content on the platform, among others.40 Violations can result in content being flagged or removed, or lead to users being blocked from the platform, all ostensibly to create a safe online environment.41 Facebook has updated its standards to target not only Islamic extremism, but also white nationalism and white separatism.42
Google’s parent company Alphabet, meanwhile, has used its Jigsaw subsidiary to pioneer The Redirect Method, which functionally serves as a targeted intervention against prospective radicalization victims whenever they seek out flagged extremist content online.\textsuperscript{43} As the project’s own descriptive page reads, “The Redirect Method...focuses on the slice of ISIS’s audience that is most susceptible to its messaging, and redirects them towards curated YouTube videos debunking ISIS recruiting themes.”\textsuperscript{44} Jigsaw employed former ISIS members to develop an understanding of prevalent extremist propaganda themes, narratives, and content, and then augmented that understanding with digital targeting tools to both flag suspected extremist content and identify countervailing media content from across the internet.\textsuperscript{45}

Both Facebook’s Community Standards and The Redirect Method are commendable at face value from a purely counter-extremism perspective. Both solutions attempt to deal with the motivated cognition problem discussed earlier by intercepting content before it reaches extremist-susceptible parties. The Redirect Method also disrupts filtering processes by redirecting individuals actively seeking engagement with online extremist communities to more moderate voices.

While commendable, both initiatives also fall short on several key components of optimal self-regulation. Facebook’s Standards are virtually entirely contrived in-house, and report only raw numbers for content that has been flagged or removed without regard to measures of effectiveness. This strategy brings the firm’s commitment to transparency and the relevance of its benchmarks into question. Moreover, Facebook does not go out of its way to report its success against its own benchmarks, which limits the potential for oversight. However, Facebook has demonstrated a receptiveness to public and Congressional demands that it do better. Its proclaimed willingness to adopt the Honest Ads Act’s provisions as well as its recent commitment to tightening restrictions on white nationalist content are both encouraging signs of increasing accountability.

The Redirect Method performs better from a self-regulatory perspective. Jigsaw developed the technology and human capital for the Redirect Method in consultation with many external think tanks and experts, and its measures of performance and effectiveness are easy to access and appear valid.\textsuperscript{46} Yet The Redirect Method is hampered by a lack of clear commitment to oversight and
accountability from the public sector or, if such oversight and accountability exists, it is not clearly outlined in public materials. More fundamentally, The Redirect Method targets victims of Islamic extremism’s radicalization efforts and does little to combat home-grown, domestic extremist movements in the United States.

Recognizing that firms’ self-regulatory efforts are imperfect is not cause for casting these efforts as either misguided or ineffective. It simply indicates an opportunity for public-private cooperation in combating online extremism and radicalization. We need the government to commit itself to regulatory approaches which complement the laudable existing efforts of these two social media giants, while also avoiding entanglements with First Amendment protections. Five recommendations are prudent.

1. **Name the threat:** Any governmental enhancement of private self-regulatory frameworks vis-à-vis online extremism and radicalization should explicitly name the threat: domestic extremist movements. A standard understanding of what constitutes domestic extremism, shared by the public and private sectors, must be adopted before any further regulatory frameworks can be implemented by the government.

2. **Enforce transparency as a consumer health issue:** The Honest Ads Act’s (HAA) most significant provision is its requirement that social media firms provide and update a public database on who purchases ads on their platforms. This is functionally equivalent to the FDA certification processes for food and drugs: it allows consumers to know that the products they are using are safe. By recasting online extremism as a matter of industrial regulation, the government can avoid allegations of censoring free speech and create social support for the HAA or equivalent legislation. The HAA or equivalent legislation should ensure that it addresses ad purchases by domestic extremist movements in addition to foreign adversaries with known histories of promoting divisive social issues online.

3. **Enforce accountability as a consumer health issue:** The Emergency Planning and Community Right-to-Know Act requires firms to report all hazardous chemicals stored and dumped to state and local governments. This approach enforces accountability by mandating negative externalities generated by private industrial practices be made accessible to the public. A similar
piece of legislation requiring social media companies to report the number of domestic extremists identified on, removed from, or redirected by their platforms would illuminate the prevalence of the threat posed by these individuals, and how effective firms are at dealing with this threat.

4. Check firms’ work: Princeton University’s Web Transparency and Accountability Project creates bots to masquerade as real people, places them online, and tracks how long it takes for those bots to suffer some form of discrimination, whether in job applications, academic admissions, or medical treatment.49 The government should mirror this practice to collect their own data on how effective firms are at meeting their own benchmarks for countering extremism on their platforms. Instead of assessing the time between a bot’s creation and its first experience of discrimination, this project would seek to identify the time and pathways to achieve radicalization. This would go a long way towards ensuring government oversight and accountability.

5. Name and subsidize good actors: Firms that voluntarily take meaningful steps towards self-regulation with the explicit purpose of combating extremism and radicalization on their platforms should be recognized and rewarded. The government should prepare a tiered system of subsidies for firms which voluntarily adopt measures, such as the HAA, which are not yet law. These subsidies should be specifically targeted to help companies implement further measures to increase their transparency, ability to create meaningful benchmarks through collaboration with external expertise, achieve governmental oversight, and ultimately create private accountability to the public welfare. Companies receiving these subsidies should be publicly reported as actively promoting the public’s health and welfare.

Companies which do not implement sufficiently rigorous self-regulatory procedures will not be penalized. They simply will not receive federal support and risk being implicitly shamed for not being interested in promoting the public’s welfare.50 Corporate self-interest should suffice to motivate desired organizational change.

---

Corporate self-interest should suffice to motivate desired organizational change.
CONCLUSION: TOWARDS A NEW SOCIAL (MEDIA) CONTRACT

The complexity of the threat posed by online extremism and radicalization to American domestic security is significant, both technologically and legally. This paper’s recommendation to refocus federal efforts through a public health lens holds the promise of employing governmental tools beyond restrictions to individual liberties, but such a paradigm shift is neither a panacea nor guaranteed smooth sailing, particularly in our current political climate. Potential points of contention are addressed below.

First, Congress is reluctant to pass new regulation, and is generally slow to do so. Even when legislators do manage to impose regulatory restrictions on large industries, exemptions and loopholes proliferate rapidly. However, regulation is still a viable option for two reasons, one philosophically idealistic while the other utterly practical. Philosophically, the mere fact that regulation is difficult ought not to preclude its use by liberal democratic law-making institutions. If Congressional leaders make the case to the public that social media platforms are contributing to the loss of American lives, there is a chance that the voters will respond with an increased demand that legislators regulate and reward those legislators who do so effectively. Practically, the recommendation to create a tiered system of subsidies for companies that voluntarily implement self-regulation is more a palatable form of regulation compared to traditional approaches: providing incentives instead of imposing restrictions.

A second point of contention is that social media companies may not get on board with self-regulation, effectively quashing the notion through collective inaction. However, our case studies suggest this is not the trend. Google and Facebook, the predominant social media players by most metrics, have clearly recognized the value of self-regulation. Their efforts, while imperfect, send a strong message from industry leaders that the status quo is unacceptable. The policy recommendations made in this paper, if adopted, will only strengthen the self-regulation regime. Moreover, the practice of naming good actors and implicitly shaming noncompliant ones (inherent in several of the legislative approaches recommended here) places pressure on recalcitrant firms if they
are perceived by customers as unsafe or untrustworthy. One need only look
at the penalty Facebook has already incurred due to customer concerns about
their privacy to understand how significant a motivator these risks can be
once the public becomes aware of them.51

The third shortcoming of these recommendations is they do not address how
law enforcement agencies might best adapt their current techniques and pro-
cedures to the digital world to identify, intervene, or apprehend online ex-
tremists. This is an important topic for further research, but it goes beyond
the scope of this paper. Nevertheless, synchronizing law enforcement’s ef-
forts with social media firms’ practices in dealing with extremism on their
platforms would be considerably easier if the measures proposed here were
adopted by Congressional leadership, in particular, the recommendation to
standardize the definition of extremism across government and the private
sector.

Ultimately, leaders across all sectors of our nation must reframe their under-
standing of the threat posed to all of us by social media-enabled radicalization.
The violence spawned by this process is real, and it threatens us all equally.
We urgently need a common acknowledgment of the duties and obligations
Americans have to one another, not merely as members of corporate or gov-
ernment entities, online tribes, or the generic “public,” but rather as common
citizens with a shared commitment to one another’s well-being and security.
Silence on this commitment from Congress and Silicon Valley will do nothing
to stanch our national bleeding; leadership on it will align our practices with
our highest aspirations and values. ■
ABOUT THE AUTHOR

Major Tony Formica graduated from the United States Military Academy at West Point in 2009 with a B.S. in International Relations and East Asian Area Studies. He commissioned as an infantry lieutenant in the U.S. Army and was first posted to Fort Wainwright, Alaska. While there, he deployed and led soldiers in Kandahar Province, Afghanistan before returning to the United States in the spring of 2012. Tony was selected as a U.S. Army Downing Scholar in the fall of 2017 and focuses his graduate studies on the national security implications stemming from the interaction of social media, economic inequality, and political tribalism.

ENDNOTES


2. For the purposes of this paper, the terms “extremist” and “extremism” will be understood by the definition used by the Federal Bureau of Investigation as entailing individuals or movements which “…[encourage], [condone], [justify], or support the commission of violent act[s] to achieve political, ideological, religious, social, or economic goals.”; Federal Bureau of Investigation, “What is Violent Extremism?,” accessed April 28, 2019, https://cve.fbi.gov/whatis/; Liam Stack, “Over 1,000 Hate Groups Are Now Active in United States, Civil Rights Group Says,” The New York Times, February 20, 2019, https://www.nytimes.com/2019/02/20/us/hate-groups-rise.html.


4. Ibid.


9. Liam Stack, “Over 1,000 Hate Groups Are Now Active in the United States, Civil Rights Group Says.”


12. Ibid, 1.


20. Andrew Guess et al., “Avoiding the echo chamber about echo chambers: Why selective exposure to like-minded political news is less prevalent than you think,” Knight Foundation, 2018, 8.


27. Ibid.


30. Ibid.


34. Ibid.


36. Ibid.

37. Ibid.

38. Ibid.

39. Ibid.


41. Ibid.


44. Sharma et al., “The Food Industry and Self Regulation.”

45. Ibid.

46. The Redirect Method.


48. Sunstein, #Republic: Divided Democracy in the Age of Social Media, 218.


50. Warner, “Warner and Klobuchar Call on Google & Twitter to Comply with the Honest Ads Act.”
