

Wirtschaft und Management

Schriftenreihe zur wirtschaftswissenschaftlichen Forschung und Praxis

Politisches Risiko neu denken: Auf der Suche nach praxisorientierten politischen Risikomodellen



Hannes Meissner
**Identifizierung und Messung spezifischer politischer Risiken in
den Ländern der östlichen Partnerschaft und Russlands**

Johannes Leitner
**Management politischer Risiken für Unternehmen.
Schwierig, aber möglich. Und wünschenswert.**

David Morris
**The Huawei paradox:
cyber-risks in a deteriorating geopolitical climate**

Beat Habegger
**Political Risk Management as an Imperative for the
Insurance Industry – and Beyond**

Elkhan Nuriyev
**Competing Regionalisms in the EU's Eastern Neighborhood:
Geopolitical Risks, Challenges and Prospects**

Gefördert von



Wirtschaft, Arbeit
und Statistik

Wirtschaft und Management

Schriftenreihe zur wirtschaftswissenschaftlichen
Forschung und Praxis

Gefördert von



**Stadt
Wien**

Wirtschaft, Arbeit
und Statistik

FH Fachhochschule
des BFI Wien
Wirtschaft
Management
Finance

AutorInnenhinweise

Möchten Sie einen Beitrag in „Wirtschaft und Management“ veröffentlichen? Wir freuen uns, wenn Sie uns einen Artikel senden und werden Sie nach besten Kräften unterstützen. Nachfolgend finden Sie einige Hinweise, um deren Beachtung wir Sie dringend ersuchen.

1. Allgemeine Hinweise

- **Dateityp:** Word-Dokument
- **Schrift:** Arial
- **Schriftgröße:** 10 Pkt.
- **Zeilenabstand:** 1,5 Zeilen
- **Satz:** Blocksatz
- **Silbentrennung:** Bedingten Trennstrich (Strg und -) verwenden
- **Rechtschreibung:** Bitte verwenden Sie die neuen deutschen Rechtschreibregeln. Es ist auf eine geschlechtsneutrale Schreibweise zu achten.
- **Bilder und Grafiken:** Stellen Sie bitte alle Bilder und Graphiken in separaten Dateien bei! Die Bildauflösung muss für den Druck mindestens 300dpi betragen. Bedenken Sie bei der Einbindung von Grafiken und Bildern, dass Ihr Beitrag im Schwarz-Weiß-Druck erscheinen wird und wählen Sie starke Kontraste und keine dunklen Hintergründe.
- **Lebenslauf und Portrait:** Stellen Sie bitte in extra Dateien einen kurzen Lebenslauf (ca. 5 bis max. 10 Zeilen) und ein Portrait von Ihnen und Ihren MitautorInnen bei (mind. 300dpi).
- **Bitte schreiben Sie im Fließtext und verwenden Sie nur Standardformate!**

2. Gestaltung des Beitrags

- **Titel des Beitrags:** fett
- **AutorIn:** Geben Sie Titel Vorname Nachname der/des Autorin/Autors sowie Institution/Firma an
- **Abstract:** Stellen Sie Ihrem Beitrag bitte einen kurzen deutschen und englischen Abstract voran.
- **Überschriften:** Verwenden Sie maximal drei Gliederungsebenen (1.; 1.1.; 1.1.1.)
- **Aufzählungen:** Nummerierte Aufzählungen mit 1., 2., 3. usw. nummerieren, Aufzählungen ohne Nummerierung nur mit vorangestelltem Trennstrich -.
- **Fett und Kursivdruck:** Nicht nur das Wort, auch die vorne und hinten angrenzenden Silbenzeichen im selben Format.
- **Anmerkungen:** Anmerkungen werden als Fußnoten notiert (Menü Einfügen / Fußnote / Fußnote Seitenende; automatische Nummerierung).
- **Zitation im Text:** Zitieren Sie nur **im** Text.
Ein/eAutorIn:(FamiliennameJahr);ZweiAutorInnen/HerausgeberInnen:(Familienname/FamiliennameJahr);
Mehrere AutorInnen / HerausgeberInnen: (Familienname et al. Jahr);
Mit Seitenangaben: (Familienname Jahr: ##) oder (Familienname Jahr: ##-##) oder (Familienname Jahr: ## f.) oder (Familienname Jahr: ## ff.).
Mehrere Literaturzitate bitte nach Erscheinungsjahr reihen und durch Strichpunkt(e) trennen.
Mehrere Literaturzitate desselben Autors / derselben Autorin mit Beistrich absetzen.
- **Literaturverzeichnis:** Das komplette Literaturverzeichnis platzieren Sie am **Ende des Textes**.
Monographie: Familienname, Vorname (Jahr): Titel. Ort: Verlag.
Zeitschrift: Familienname, Vorname (Jahr): Titel. In: Zeitschrift Vol (Nr.), ##-##.
Zeitung: Familienname, Vorname (Jahr): Titel. In: Zeitung Nr., Datum, ##-##.
Internet-Dokument: Familienname, Vorname (Jahr): Titel. <URL>, Datum des Download (= last visit).
Sammelbände: Familienname, Vorname/Familienname, Vorname (Hg. bzw. ed./eds., Jahr): Titel. Ort: Verlag.
Aufsätze in Sammelbänden: Familienname, Vorname (Jahr): Titel. In: Familienname, Vorname (Hg. bzw. ed./eds.): Titel. Ort: Verlag, ##-##.
Mehrere AutorInnen: Familienname, Vorname/Familienname, Vorname (Rest siehe: ein/e AutorIn)

3. Betreuung durch die Redaktion / Nutzungsrechte

Bitte stimmen Sie Thema und Länge Ihres Beitrags mit der Redaktion ab. Die Redaktion steht Ihnen gerne für Fragen bzw. zur Abstimmung Ihres Themas zur Verfügung. Mit der Einreichung des Manuskripts räumt der/die AutorIn dem Herausgeber für den Fall der Annahme das unbeschränkte Recht der Veröffentlichung in „Wirtschaft und Management“ (in gedruckter und elektronischer Form) ein. Vor der Veröffentlichung erhalten Sie die redigierte Endfassung Ihres Beitrags zur Freigabe. Sie werden ersucht, diese Version rasch durchzusehen und die Freigabe durchzuführen. Notwendige Korrekturen besprechen Sie bitte mit der Redaktion. Nach Erscheinen Ihres Artikels erhalten Sie 5 AutorInnenexemplare durch den Herausgeber. Mit der Übermittlung des Manuskripts erkennen Sie die Bedingungen des Herausgebers an. Die AutorInnenhinweise sind einzuhalten.

Kontakt: Katharina Becker BA MA; E-Mail: katharina.becker@fh-vie.ac.at; Tel.: +43/1/720 12 86-66
Fachhochschule des BFI Wien, Wohlmutstraße 22; 1020 Wien



Andreas Breinbauer
Leiter des FH-Kollegiums der
Fachhochschule des BFI Wien

Editorial

Sehr geehrte Leserin, sehr geehrter Leser!

Ich freue mich, Ihnen die aktuelle Ausgabe unserer Schriftenreihe unter dem Titel „Politisches Risiko neu denken: Auf der Suche nach praxisorientierten politischen Risikomodellen“ präsentieren zu dürfen, die im Rahmen des, von der **Stadt Wien** geförderten, **Forschungsprojekts STRATOS** – „*Strategisches Management Politischer Risiken in der Östlichen Partnerschaft und Russland für Österreichs Unternehmen*“ entstanden ist.

In den letzten Jahren ist die internationale Öffentlichkeit Zeuge enormer politischer und sozioökonomischer Veränderungen und Herausforderungen geworden. Deren Ursachen sind komplex und nur einige von ihnen können mit bestimmten Ländern und/oder Regionen in Verbindung gebracht werden. Dennoch sind die Auswirkungen in unserer hochintegrierten Welt weitreichend. Für multinationale Unternehmen (MNEs) ist das globale Umfeld daher unsicherer geworden. Folglich benötigen MNEs mehr denn je geeignete Strategien, wie mit diesen politischen Risiken umzugehen ist und ein besseres, praxisorientiertes politisches Risikomanagement.

Das wirft die Frage auf, ob, wie und in welchem Umfang die Forschung dazu beitragen kann. Der akademische Diskurs dazu ist sehr heterogen und im Vergleich zu anderen Bereichen noch unterentwickelt. Das Interesse und die methodische Charakteristik der Wirtschaftswissenschaften bestimmen die politische Risikoliteratur. Dies führt mitunter zur Dominanz hochkomplexer quantitativer/ökonometrischer Studien, die sich auf bestehende Modelle stützen, um die Bedeutung einzelner politischer Risikofaktoren zu testen. Dieser Ansatz ist mit einem Mangel an qualitativen, in die Tiefe gehenden Kontextstudien und praxisorientierten politischen Risikomanagementmodellen verbunden, die von MNEs angewendet werden können.

Vor diesem Hintergrund zielt diese Ausgabe von „Wirtschaft und Management“ darauf ab, politische Risiken zu überdenken. Es geht darum, eine offene Diskussion darüber zu führen, wie das politische Risikomanagement in der Praxis abläuft bzw. ablaufen könnte. Wie können ForscherInnen, AnalystInnen und WirtschaftsvertreterInnen politische Risiken in der Praxis identifizieren, analysieren und managen?

Wie gehen sie mit dem Spannungsverhältnis zwischen der Komplexität des politischen und sozio-ökonomischen Umfelds, in dem die Unternehmen einerseits operieren, und andererseits der Realität des Daily Business um?

Der erste Beitrag stammt von **Hannes Meissner** und weist zu Beginn auf den steigenden Bedarf an politischem Risikomanagement hin. Anschließend diskutiert der Autor die Praxistauglichkeit von Forschungsansätzen und Modellen für Unternehmen und zeigt Grundzüge eines bedarfsorientierten Analysemodells auf.

Im zweiten Beitrag erörtert **Johannes Leitner** die Defizite in der Praxis des Managements politischer Risiken und zeigt vier Strategien auf, die Unternehmen beim Managen politischer Risiken zur Verfügung stehen.

Bezugnehmend auf die Thematik der Cyber-Risiken, erläutert **David Morris** im dritten Beitrag anhand des Unternehmens Huawei, welche Auswirkungen politische Cyber-Risiken auf Bereiche der internationalen Sicherheit, Wirtschaft und Beziehungen haben und welche Maßnahmen zur Risikovermeidung und zum Risikomanagement gesetzt werden können.

Beat Habegger beschäftigt sich im vierten Beitrag mit der Frage, inwieweit Versicherungen mit politischen Risiken konfrontiert sind und wie sie diese entsprechend analysieren und managen können. Zudem wird aufgezeigt, was andere Unternehmen von der Versicherungsbranche lernen können.

Im abschließenden fünften Beitrag geht es um konkurrierende Regionalismen und die Frage, wie sich diese Unterschiede auf die Länder der Östlichen Partnerschaft auswirken. **Elkhan Nuriyev** erläutert zudem die aktuelle Komplexität im Beziehungsgefüge EU-Russland-China und betont, dass es dringend notwendig ist, ein neues kooperatives Verhältnis auszuarbeiten.

Mein besonderer Dank gilt Johannes Leitner und Hannes Meissner, die im Zuge des Forschungsprojekts STRATOS maßgebend zur Entstehung und Herausgabe dieser Ausgabe beigetragen haben.

Ich wünsche Ihnen, geschätzte Leserinnen und Leser, eine spannende Lektüre!

Wir freuen uns auf Ihr Feedback!

Ihr



Prof. (FH) Dr. Andreas Breinbauer
Rektor (FH) der Fachhochschule des BFI Wien
andreas.breinbauer@fh-vie.ac.at

Inhaltsverzeichnis

Beiträge	Seite
Identifizierung und Messung spezifischer politischer Risiken in den Ländern der östlichen Partnerschaft und Russlands <i>Hannes Meissner</i>	7
Management politischer Risiken für Unternehmen. Schwierig, aber möglich. Und wünschenswert. <i>Johannes Leitner</i>	17
The Huawei paradox: cyber-risks in a deteriorating geopolitical climate <i>David Morris</i>	29
Political Risk Management as an Imperative for the Insurance Industry – and Beyond <i>Beat Habegger</i>	51
Competing Regionalisms in the EU's Eastern Neighborhood: Geopolitical Risks, Challenges and Prospects <i>Elkhan Nuriyev</i>	63
Verzeichnis der AutorInnen	Seite
Verzeichnis der AutorInnen	79
Working Papers und Studien der Fachhochschule des BFI Wien	Seite
Working Papers und Studien der Fachhochschule des BFI Wien	81

Impressum

Medieninhaber, Herausgeber und Verleger:

Fachhochschule des BFI Wien Gesellschaft m.b.H.
A-1020 Wien, Wohlmutterstraße 22, Tel.: +43/1/720 12 86
E-Mail: info@fh-vie.ac.at
<http://www.fh-vie.ac.at>

Geschäftsführung:

Mag.^a Eva Schießl-Foggensteiner

Redaktion:

Prof. (FH) Dr. Andreas Breinbauer
Katharina Becker, BA MA
Martina Morawetz-Wiesinger

Lektorat:

Dr. Günter Strauch
Firma Fox Coffey

Layout und Druck:

Claudia Kurz, A-2392 Grub im Wienerwald

ISBN: 978-3-902624-59-8 (Printversion)
ISBN: 978-3-902624-60-4 (Online-Version)

Hinweis des Herausgebers:

Die in „Wirtschaft und Management“ veröffentlichten Beiträge enthalten die persönlichen Ansichten der AutorInnen und reflektieren nicht notwendigerweise den Standpunkt der Fachhochschule des BFI Wien.

Hannes Meissner

Identifizierung und Messung spezifischer politischer Risiken in den Ländern der östlichen Partnerschaft und Russlands¹



Hannes Meissner
FH des BFI Wien

Abstract

Auf globaler Ebene wie im Raum der östlichen Nachbarschaft der EU und Russland nehmen politische Risiken für MNEs zu. Vor diesem Hintergrund steigt die Bedeutung von politischem Risikomanagement. Die wissenschaftliche Forschung zur Thematik hat jedoch kaum anwendungsorientierte Modelle hervorgebracht.

Vorliegender Beitrag zeigt den steigenden Bedarf an Politischem Risikomanagement zunächst auf. Im nächsten Schritt wird dargelegt, dass die hochkomplexen Forschungsansätze und Modelle sich für Unternehmen nur selten als praxistauglich erweisen. Demgegenüber werden im dritten Schritt Schlussfolgerungen hinsichtlich der Grundzüge eines bedarfsorientierten Analysemodells gezogen.

Political risks for MNEs are on the rise, globally as well as in the eastern neighbourhood of the EU and in Russia in particular. Consequently, there is a rising need for practice-oriented political risk management tools. The academic field of political risk research, however, is characterised by a lack of such models, since highly sophisticated quantitative/econometric studies dominate this field.

This contribution first analyses the rising importance of political risk management. Secondly, it demonstrates that the highly complex research approaches and models are hardly ever suited to business practice. Finally, conclusions are offered in regards to practice-oriented political risk management models that MNEs can apply.

1 Einleitung

Die Welt ist unsicherer geworden. So trivial diese Feststellung auf den ersten Blick erscheinen mag: Bei genauer Betrachtung lässt sich in der globalen Risikokonstellation eine Vielzahl an Bereichen ausfindig machen, in denen sich die Rahmenbedingungen für wirtschaftliche Tätigkeiten im letzten Jahrzehnt teils fortlaufend und absehbar, teils abrupt und überraschend verschlechtert haben. Dabei gilt grundsätzlich erst einmal festzustellen, dass es im natürlichen Lauf der Dinge liegt, dass sich politische, soziale und ökonomische Konstellationen fortdauernd verändern. Solche Entwicklungsprozesse verlaufen nicht geradlinig, sondern sind vielmehr

¹ Dieses Working Paper entstand im Rahmen des Forschungsprojekts STRATOS, das durch die MA 23 der Stadt Wien finanziell gefördert wird.

Gefördert von



Stadt
Wien

Wirtschaft, Arbeit
und Statistik

Gegenstand widersprüchlicher, gegenläufiger und/oder sprunghafter Bewegungen. Die Ursachen sind wiederum komplex und vielschichtig und können in der globalisierten Welt nur selten mit einzelnen Staaten und Regionen in Verbindung gebracht werden.

Diese Feststellung gilt nicht nur in globaler Perspektive, sondern gerade auch für die für deutsche, österreichische und Schweizer Unternehmen nach wie vor wichtige Region der östlichen Nachbarschaft der EU (Belarus, Ukraine, Moldawien, Aserbaidschan, Armenien und Georgien) sowie für Russland. Seit Auflösung der Sowjetunion zeichnete sich die Region zu allen Zeiten durch weitreichende politische Risiken aus, bei gleichzeitig unterschiedlichen landesspezifischen Ausprägungsformen. Gescheiterte rechtsstaatliche Transformationsprozesse, State-Capture Erscheinungen und die damit verbundene Überdominanz informeller Strukturen und Praktiken erweisen sich regelmäßig als schwierig zu managende politische Risikofaktoren.

Zeitgleich mit der Zuspitzung der globalen Risikokonstellation haben sich Klima und Unternehmensumfeld auch in der Region in der letzten Dekade weiter deutlich verschlechtert. Als Critical Juncture erwies sich dabei der Ukraine-Konflikt, der durch den geopolitischen Wettstreit zwischen Russland und der EU bzw. USA in der Region ausgelöst wurde. Dieser hat nicht nur einzelne Länder, sondern auch die Region als Ganzes weiter destabilisiert. Als besonders gravierend erweisen sich dabei die EU Sanktionen gegen Russland bzw. die russischen Gegensanktionen.

Vor diesem Hintergrund ist die Bedeutung politischen Risikomanagements zuletzt weiter deutlich gestiegen. Vorliegender Beitrag zeigt den Bedarf zunächst auf, wobei der Fokus nicht ausschließlich auf Russland und die Region der östlichen Partnerschaft der EU gerichtet ist, sondern vielmehr globale Entwicklungen umrissen werden. In einem nächsten Schritt wird dargelegt, dass dem steigenden Bedarf an angewandten politischen Risikoanalyse- und Risikomanagementmodellen ein fragmentierter Forschungsbereich gegenübersteht, dessen hochkomplexe Forschungsansätze und Modelle sich für Unternehmen nur selten als praxistauglich erweisen. Dem sollen im dritten Schritt Schlussfolgerungen hinsichtlich der Grundzüge eines bedarfsorientierten Analysemodells entgegengestellt werden, wobei sich vorliegender praxisorientierter Beitrag auf grundlegende Rückschlüsse bezüglich wichtiger Analyseschritte beschränkt.

2 Steigende Bedeutung politischen Risikomanagements

In der globalen Gesamtkonstellation ist der Rolle Chinas in den vergangenen Jahren besonders viel Aufmerksamkeit zuteilgeworden. Ausschlaggebend ist, dass der wirtschaftliche Aufstieg des Landes zu einer neuen geopolitischen Stärke des Landes geführt hat. Insbesondere seit Xi Jinpings Amtseinführung in 2012 setzt China die gewonnene Macht verstärkt dazu ein, die Spielregeln globaler Interaktionen im eigenen Sinn umzuschreiben. Für viele Beobachter kam das überraschend, denn in der Vergangenheit wurden dem Land sozioökonomische Entwicklungsinteressen und weniger hegemoniale Aspirationen zugeschrieben. Die fortschreitende wirtschaftliche Entwicklung des Landes würde – so der lange dominierende Glaube – politische

Reformen induzieren und eine immer stärkere Einbindung des Landes in tradierte westliche Wirtschaftsstrukturen bewirken. Doch es kam anders. Das autoritäre Herrschaftssystem des Landes ist mehr denn je gestärkt, und die wirtschaftliche Öffnung des Landes für ausländische Unternehmen wird von niedrigem Ausgangsniveau beginnend weiter zurückgenommen. Handelskonflikte und der Konflikt um Taiwan und Hongkong stehen dabei geradezu exemplarisch für die Krise der liberalen Weltordnung.

Für lange Zeit stand die fortschreitende Globalisierung als Garant für den Abbau von Handelsbarrieren. Das Scheitern der Freihandelsabkommen TPP und TTIP und neue Handelsbarrieren zwischen China und den USA stehen heute für eine neue Ära der internationalen Beziehungen. Die Amtseinführung Donald Trumps in den USA markierte eine weitere Zäsur. Der Rückzug der USA aus dem Atomdeal mit dem Iran und der politische Kampf der US-Administration gegen das Nordstream2-Projekt werden jeweils mittels der wirtschaftlichen Übermacht des Landes geführt. Der Kollateralschaden liegt derweil bei beteiligten Unternehmen, die sich mit Sanktionen konfrontiert sehen und sich aufgrund der Bedeutung des US-Marktes von betroffenen Projekten letztlich zurückziehen müssen. In welchem Bereich und inwieweit John Biden mit dieser Politik brechen wird, bleibt abzuwarten. Ein Zurück zu alter Vertrautheit und Berechenbarkeit wird es in den Beziehungen Europas zu den USA kaum mehr geben.

Der Einfluss der USA darf jedoch nicht darüber hinwegtäuschen, dass sowohl die USA als auch die EU im globalen Wettstreit mit China schwächer positioniert sind, als sie es zu Zeiten des Ost-West-Konfliktes gegenüber der Sowjetunion waren. Die damalige wirtschaftliche Übermacht des Westens und das damit verbundene Wohlfahrtsversprechen mündeten in den 90er Jahren in Osteuropa in den Siegeszug neoliberaler Marktprinzipien. Doch knapp 30 Jahre später ist die Position des Westens durch die Schuldenkrise, die Migrationskrise, die wachsende Schere zwischen armen und reichen Menschen und Ländern und den daraus resultierenden Zulauf zu populistischen Bewegungen geschwächt. Dies gilt insbesondere für die EU, welche zur Gefangenen ihrer selbst geworden ist. Dem Bedarf, mittels weitreichender Integrationsschritte die strukturellen Ursachen ihrer institutionellen und Finanz/Euro-Krise zu überwinden, steht der Aufstieg populistischer Bewegungen in einigen Mitgliedstaaten gegenüber, welche einfach gestrickte Re-Nationalisierungsideen als Allheilmittel gegen die Krise verkaufen. Sezessionistische Bewegungen wie in Katalonien und Schottland, der BREXIT, der Einfluss korrupter, halb-autoritärer EU-kritischer Regierungen in Polen und Ungarn haben sich derweil als gravierende politische Risiken für MNEs herausgestellt. Wohlgedenkt, dies geschieht in den bislang als sicher geltenden Heimatmärkten und eben nicht in Schwellenländern.

Auf Länderebene ist eine neue Welle des Autoritarismus zu beobachten. Dies gilt nicht nur für China und Mittelosteuropa, sondern auch für den Nahen Osten, wo der sogenannte Arabische Frühling gescheitert ist, von Tunesien einmal abgesehen. Letztlich war nach einer kurzen Phase der Liberalisierung ein Wiederaufstieg von Militärregimen zu beobachten (Syrien, Ägypten). Andere Länder sind dagegen ganz in Krieg, Chaos und Terrorismus abgeglitten (Libyen, Syrien, Irak). Derweil nützen autoritäre Herrschaftssysteme im postsowjetischen Raum die

Geschehnisse neuerlich zur Legitimierung ihrer Macht, indem sie das Stabilitätsparadigma betonen, welches die Vorteile autoritärer Stabilität hervorhebt. Autoritäre und korrupte Eliten verkaufen sich als Garanten von Sicherheit und Ordnung. Demokratisierungsbestrebungen werden als gefährliche Experimente dargestellt, welchen Instabilität und Chaos inhärent ist. In traditionellen paternalistischen Gesellschaften mit fehlender demokratischer Tradition fallen solche Argumente dabei auf fruchtbaren Boden.

Im postsowjetischen Raum ist das sogenannten Transformationsparadigma gescheitert. Als diese Länder 1991 ihre Unabhängigkeit erlangten, ging man noch davon aus, dass sie sich praktisch automatisch in Richtung Demokratie und Rechtsstaatlichkeit (und Marktwirtschaft) bewegen würden. Tatsächlich haben sich aber sogenannte State-Capture Konstellationen verfestigt, die sich dadurch auszeichnen, dass herrschende Eliten (Clans, Businesszirkel, Oligarchen, Familien- und Freundschaftsnetzwerke) ihre Machtposition ganz für ihr privates Interesse ausnützen. Die Folgen sind gravierende politische Risiken wie institutionelle Defizite, eine nicht nach rationalen Kriterien funktionierende Bürokratie, Klientelismus, Rechtsunsicherheit und Defizite hinsichtlich der Gewährung der Eigentumsrechte (cf. Leitner/Meissner 2016).

Im postsowjetischen Raum tritt ein weiterer politischer Risikofaktor hinzu, der im Zusammenhang mit einem neuen Kapitel des traditionellen geopolitischen Wettstreits zwischen der Hegemonialmacht Russland, den USA und der EU steht. Das Ende des Kalten Krieges ist in keine neue europäische Sicherheitsordnung gemündet. Vielmehr sind EU und NATO in jenen geographischen Raum vorgerückt, der zuvor allein durch Moskau kontrolliert wurde. Nach Vladimir Putins Machtübernahme ist diese Politik zunehmend auf den Widerstand Russlands getroffen. 30 Jahre nach Ende des Kalten Krieges ist heute wieder von einem „Neuen Kalten Krieg“ die Rede. Bereits 2008 setzte der Augustkrieg den unter Präsident Mikheil Saakashvili vorangetriebenen Aspirationen Georgiens hinsichtlich einer NATO- und EU-Mitgliedschaft ein jähes Ende. Seit 2014 steht die Ukraine im Mittelpunkt dieser geopolitischen Auseinandersetzung. Die Folgen der Euro-Maidan-Revolution, die nachhaltige Destabilisierung des Landes, der Kontrollverlust über die Krim und die Ostukraine und mehr noch die Sanktionen der EU gegen Russland und die russischen Gegensanktionen stellen regionalspezifische politische Risikofaktoren mit gravierenden Auswirkungen auf MNEs dar.

Die Geschehnisse in der Ostukraine, der Augustkrieg 2008 und die jüngste dramatische Eskalation des Konfliktes zwischen Armenien und Aserbaidschan um Bergkarabach beweisen derweil, dass die sogenannten „frozen conflicts“ auf dem postsowjetischen Territorium weniger eingefroren sind, als dies lange wahrgenommen wurde. Für MNEs stellen die international nicht anerkannten sogenannten „Defacto-Republiken“ (Südostsetien, Abchasien, Bergkarabach, Volksrepubliken Lugansk und Donezk) dabei nicht nur No-Go Areas dar, sie bilden auch mehr oder weniger undurchlässige Barrieren für Logistik- und Handelsrouten. Dies gilt allerdings weniger für Transnistrien, das über die Republik Moldau Möglichkeiten einer besseren Einbettung in internationale Handelsstrukturen zu nutzen weiß.

Autoritäre Herrschaft ist darüber hinaus mit Reputationsrisiken für MNEs verbunden. Der Volkswagen-Fall in der westchinesischen Provinz Xinjiang ist ein klassisches Beispiel hierfür. Im Jahr 2019 wurde die Firma der Komplizenschaft mit dem chinesischen Regime beschuldigt, nachdem sie angegeben hatte, über die Internierung der Uiguren nichts zu wissen, obwohl sie in der Region eine Fabrik unterhält (Noack/The Washington Post 2019).² In einem weiteren Fall wurde der schwedische Mobilfunkbetreiber TeliaSonera der Korruption und Begünstigung der aserbaidischen Herrscherfamilie beschuldigt (Hellstrom/Reuters 2015). In einem solchen Kontext sehen sich betroffene MNEs mit ethischer Kritik konfrontiert. Unethisches Verhalten manifestiert sich in einem ausländischen Markt häufig entlang von Korruption, Menschenrechtsverletzungen und Umweltschäden. Dies bewirkt letztlich gesellschaftliche Widerstände, Opposition durch soziale Bewegungen und eine schlechte Medienberichterstattung. Im Fall tatsächlich begangener Rechtsverletzungen werden Missstände mittels sozialer Bewegungen und sozialer Medien heute schneller und leichter aufgedeckt als in der Vergangenheit, was vor dem Hintergrund strikterer Compliance Vorschriften Rechtsverfahren nach sich ziehen kann.

3 Defizite der politischen Risikoforschung – mangelhafte Praxistauglichkeit der Ansätze

In der politischen Risikoforschung haben Reputationsrisiken und gesellschaftliche Faktoren nur bedingt und erst in jüngerer Zeit eine gewisse Berücksichtigung gefunden. Eine Auseinandersetzung mit der Thematik findet allenfalls in der Literatur zu Stakeholder-Management und Non-Market-Strategien statt. Das Hauptaugenmerk der politischen Risikoforschung liegt traditionell auf politischen Ereignissen, häufig in Verbindung mit Konflikten und Kriegen und der Politikgestaltung durch Regierungen. Vorliegend soll daher eine weite Definition von Politischem Risiko gewählt werden. "Political risks comprise any occurrence in the international business context where public actions or non-state actors that are active in the host country of the international activities interfere with private international businesses and adversely impact the performance of the international operation." (Leitner 2017)

Insgesamt ist das gesamte Forschungsfeld heterogen und unterentwickelt, obwohl der politischen Risikoforschung wachsende Aufmerksamkeit zuteil wird. Es ist dabei fast ausschließlich in der Disziplin der International Business Studies verankert, während die Thematik in der Politikwissenschaft nach wie vor keine größere Rolle spielt, obwohl es durchaus einige Forschungsbemühungen mit politikwissenschaftlichem Bezug gibt (Alon/Matthew 1998; Alon/Herbert 2009; Sottilotta 2013; Jensen/Young 2008; Jensen 2002; Jensen et al. 2014; Hellmann et al. 2000). In der Folge dominieren Interesse und Methoden der Business Studies die Forschungsliteratur. Im Endergebnis überwiegen quantitative, ökonometrische Modelle, welche bestehende Modelle aufgreifen, um die Signifikanz einzelner eng definierter politischer Risikofaktoren auf Unternehmensperformance zu testen (cf. Graham et al. 2015).

² The Washington Post (2019) von Rick Noack stellt hierzu fest: "As a company rooted in Nazi Germany, German car manufacturer Volkswagen might be expected to have a somewhat more sensitive approach to ethics than its competitors. But Volkswagen has acquired a reputation in recent years for pursuing practices condemned as unethical by authorities and critics." (Washington Post 2019)

Das Erkenntnisinteresse ist dabei rein wissenschaftsgetrieben. Es geht letztlich nicht darum, anwendungsorientierte Modelle für Unternehmen zu entwerfen.

Trotz einiger weniger Ansätze (Alon/Matthew 1998, Sottilotta 2015) mangelt es gleichzeitig insgesamt an tiefgreifenden und umfassenden Kontextmodellen, die darauf gerichtet sind, ein sozioökonomisches Umfeld in der vollen Dimension und Wirkung zu erfassen. Solche Ansätze sind eher in der Politikwissenschaft beheimatet. Lediglich wenige Studien sind darauf gerichtet, die volle Komplexität hinsichtlich der Wirkungszusammenhänge einzelner Variablen (z.B. das Rechtssystem, Czinkota/Skuba 2014; politischer Konflikt, Henisz et al. 2010) oder mehrerer Variablen (vgl. Governance und State Capture, Hellmann et al. 2000) abzubilden.

Vor diesem Hintergrund zeichnet sich die gegenwärtige Literatur durch drei thematische Trends aus. Ein erster Literaturblock beschäftigt sich mit den Auswirkungen von Korruption auf Investitionsbedingungen und Unternehmenstätigkeiten (vgl. Zucker Boswell 1999, Grandel/Teixeira 2012). In diesem Zusammenhang untersuchen einige Studien Markteintrittsstrategien, wobei die Frage darauf gerichtet ist, ob Unternehmen unter diesen Bedingungen eher die Gründung von Tochtergesellschaften oder Franchise Modelle präferieren. Der zweite Literaturblock untersucht die Unterschiede zwischen OECD-Ländern und Schwellenländern hinsichtlich politischer Risikokonstellationen und Geschäftschancen (vgl. Brouthers 1995, Diamonte et al. 1996). Dabei ist zu betonen, dass politische Risikobewertungen häufig auf subjektiver Basis stattfinden, wobei kognitiven Aspekten und der Unternehmenskultur ein entscheidender Einfluss zukommt. Während einige ManagerInnen bestimmte Faktoren als Risiko betrachten, was zur Entscheidung gegen einen Markteintritt führt, halten genau die gleichen Faktoren andere ManagerInnen nicht von diesem Schritt ab. Der dritte Literaturblock setzt sich mit den Konsequenzen von Demokratie vs. Autoritarismus für MNEs auseinander. Signifikanter Weise kommen diese Studien zu widersprüchlichen Ergebnissen (vgl. Olson 1993, Haggard 1990, Li/Reuveny 2003: 176). Hieran erschließt sich neuerlich der Bedarf an in die Tiefe gehenden landesspezifischen Kontextmodellen, denn hochaggregierte Daten, welche Länderisikoindizes miteinander kombinieren und zueinander messen, tendieren häufig zu einer verkürzten Abbildung der Realität.

Wie Jensen et al. (2014) feststellen, "there is wide variation in the institutional architecture of authoritarian regimes, and that these differences have important implications for economic performance and domestic investment." (Jensen et al. 2014: 655/656) Neben institutionellen Eigenheiten fallen auch unterschiedliche persönliche Interessen der Autokraten ins Gewicht. Einige autoritäre Herrscher sind möglicherweise stärker an FDIs interessiert als andere. Unterschiedliche Effekte können auch auf die Form und die Höhe der Investition zurückgehen. Auch der Wirtschaftssektor kann ausschlaggebend sein. Wenn wir als Beispiel die drei autoritären Staaten China, Nordkorea und Venezuela heranziehen, ist sofort augenfällig, dass sich diese in vielen Kontextvariablen unterscheiden, wie die Ausprägungsform und Stärke des autoritären Regimes, interne und externe Konflikte, Regierungsinteressen und die Einbeziehung des Landes in globale Handelsstrukturen.

4 Anwendungsorientierte Analyseschritte

Im Zuge des STRATOS Projektes³ entwickelt das Kompetenzzentrum Schwarzmeerregion an der FH des BFI Wien politische Risikomanagement-Tools speziell für Unternehmen, die in der östlichen Partnerschaft der EU und in Russland operieren oder einen Markteintritt planen. Hierfür wurden Umfragen unter deutschen, österreichischen und Schweizer Unternehmen an ihren Headquarters durchgeführt (2016-2019) sowie Feldforschung in Russland, Kasachstan und Usbekistan betrieben (2018-2019). Im Ergebnis offenbarte sich neuerlich, dass der Anwendung von politischen Risikomanagement-Tools zwei entscheidende Schritte vorgelagert sind: die umfassende Identifikation und die Analyse politischer Risiken.

Die Schritte müssen gleichzeitig in die Breite und die Tiefe gerichtet sein, das heißt, sie müssen die volle Dimension des möglichen Impacts der politischen Risikofaktoren/Risikokonstellation auf ein Unternehmen bzw. Unternehmensprojekt erfassen. Aus Sicht von ManagerInnen mag dies selbstverständlich erscheinen. Tatsächlich sind jedoch nicht nur Forschungsinteressen zumeist anders gelagert, sondern Risikoberater in staatlichen Institutionen wie privaten Unternehmen sehen ihre Aufgabe und Geschäftschance nicht selten darin, vergleichsweise allgemein gehaltene Reports auf Länderebene zu verkaufen.

Hierin darf sich jedoch politische Risikoberatung nicht erschöpfen. Tatsächlich liegt ihr eigentlicher Mehrwert darin, sehr spezifische Antworten auf Detailfragen zu einer Projekt- und Unternehmenskonstellation zu liefern. Sie ist immer dann gefragt, wenn die unternehmensinterne Expertise nicht mehr ausreicht bzw. eine objektive Bewertung identifizierter Risikokonstellationen durch eine außenstehende Partei erforderlich ist. Um an dieser Stelle an den aktuellen Forschungsdiskurs anzuknüpfen: Für Unternehmen sind makropolitische Risikoanalysen meist weniger relevant. Diese untersuchen die für alle Unternehmen gleich geltende Länderrisikokonstellation. Es geht vielmehr um sogenannte mikropolitische Risikoanalysen, das heißt, um Untersuchungen von politischen Risiken auf Unternehmens- bzw. Projektebene.

Derartige vielfach eher schwache Beratungsleistungen mögen ihren Teil dazu beigetragen haben, dass der gesamte Dienstleistungsbereich der politischen Risikoberatung im deutschsprachigen Raum bislang nur schwach verankert ist. Bei vielen ManagerInnen dominiert die Sichtweise, nach Jahren operativer Tätigkeiten in politisch schwierigen Märkten ausreichend eigene Expertise angesammelt zu haben bzw. durch lokale Sales-RepräsentantInnen umfassend informiert zu werden. Tatsächlich führt dies zu einer Verengung der Perspektive, wodurch entscheidende Expertise außen vor bleibt. Gerade im Hinblick auf Sales-RepräsentantInnen ist offensichtlich, dass die Informationsvermittlung durch diese einer durch materielle Eigeninteressen bewirkten Selektion bzw. einem Bias unterliegt. Im Ergebnis gehen im besten aller schlechten Fälle Geschäftsoportunitäten verloren – im schlimmsten Fall treten Schäden ein. Gerade Märkte mit einer hohen politischen Risikokonstellation zeichnen sich zugleich

3 Das Projekt wird durch die Stadt Wien gefördert. Mehr Infos unter: <https://ccbsr.fh-vie.ac.at/stratos>.

durch hohe Geschäftschancen aus. Doch sind geschäftsschädigende Ereignisse erst einmal eingetreten, werden die betroffenen Länder von da an als zu schwierig und riskant abgetan. Grundsätzlich ist festzustellen, dass auch „Avoidance“ eine politische Risikomanagementstrategie ist. Allerdings werden mögliche „Mitigation-Strategien“ (Stakeholder Management, Best Practise Analysen, Portfolio Management, Political Strategies, Political Risk Due Diligence, Project Investigation, Compliance Investigation etc.) bzw. „Transfer-Strategien“ (Versicherungen, Outsourcing, Decoupling) nicht mehr ausreichend in Betracht gezogen.

Mit anderen Worten: Jeder Risikoanalyse geht der entscheidende Schritt der Identifikation von politischen Risiken voraus. Und hierfür ist wiederum ausreichendes Problem-(Lösungs)-Bewusstsein Vorbedingung. Eine an der Unternehmens- bzw. Projektperspektive ansetzende politische Risikoanalyse bedarf im nächsten Schritt der Fokussierung auf unterschiedliche Analyseebenen. Die erste Analyseebene ist geographischer Natur. Hier ist eine Unterscheidung zwischen globalen, regionalen, länderspezifischen und lokalen Risikofaktoren/Risikokonstellationen zu treffen. Die zweite Analyseebene betrifft die Akteursebene, wobei hier grob zwischen Regierungsakteuren/der herrschenden Elite, der Bürokratie, Nicht-Regierungsorganisationen und der Bevölkerung zu unterscheiden ist. Die dritte Analyseebene bezieht sich auf die Institutionen, wobei zwischen formalen Institutionen und informellen Institutionen und Regeln zu unterscheiden ist. Gerade letztere Dimension erweist sich regelmäßig als mit hohen Risiken behaftet, da der Umgang mit „ungeschriebenen Gesetzen“ tiefe Einblicke in den Landeskontext erfordert und die dabei in Erscheinung tretenden Praktiken vielfach im Widerspruch zu internationalen Compliance-Vorschriften stehen.

Im Endergebnis lassen sich dann auf konkrete Risikoszenarien zugeschnittene politische Risikostrategien entwerfen. Welche der oben genannten Strategien in welcher Weise und welcher Kombination zum Einsatz kommen, steht dabei im engen Zusammenhang mit den einzelnen Analyseebenen. Während auf regionaler und globaler Ebene tendenziell eher Best-Practise Analysen, Political Strategies und Political Risk Due Diligence zum Einsatz kommt, sind auf Länderebene bzw. lokaler Ebene im Umgang mit Nicht-Regierungsorganisationen und der Bevölkerung Stakeholder-Management-Strategien besonders gefragt. Auf Länderebene bieten sich zudem Decoupling-Stratgien und Versicherungen an. Stehen informelle Institutionen im Mittelpunkt der Risikoanalyse, sind Project Investigation und Compliance Investigation unverzichtbare Tools.

5 Schlussfolgerungen

Mit Blick auf die globalen Entwicklungen im Allgemeinen und die politische und sozioökonomische Situation in Russland und in der östlichen Nachbarschaft der EU spricht vieles dafür, dass sich die politische Risikokonstellation für MNEs in den nächsten Jahren kaum entspannen wird. In vielen Bereichen dürften sich die eingangs skizzierten Problemlagen vielmehr verschärfen. Damit steigt der Bedarf an politischen Risikomanagement-Tools für Unternehmen.

Ob sich dieser Forschungsbereich im deutschsprachigen Raum weiter verankern wird, hängt jedoch stark davon ab, ob eine Überwindung disziplinärer Trennlinien zwischen International Business Studies und Politikwissenschaft im größeren Umfang gelingt und ob die Fachhochschulen ausreichend Initiative zeigen, das Forschungsfeld aus dem engen Bereich rein wissenschaftsgetriebener Forschung in den Bereich angewandter Forschung zu transferieren. Das STRATOS Projekt am Kompetenzzentrum Schwarzmeerregion der FH des BFI Wien ist hierfür ein entscheidender Schritt.

6 Literaturverzeichnis

Alon, Ilan / Herbert, Theodore T. (2009): A Stranger in a Strange Land. Micropolitical Risk and the Multinational Firm. In: *Business Horizons*, 52(2), 127-137.

Alon, Ilan / Martin, Matthew A. (1998): A Normative Model of Macro Political Risk Assessment. In: *Multinational Business Review*, Vol. 6 Fall, 10-19.

Brouthers, Keith D. (1995): The influence of international risk on entry mode strategy. In: *Management International Review*, 35(1), 7-28.

Czinkota, Michael R. / Skuba, Charles J. (2014): Contextual analysis of legal systems and their impact on trade and foreign direct investment. In: *Journal of Business Research*, 67(10), 2207-2211.

Diamonte et al. (1996): Political Risk in Emerging and Developed Markets. In: *Financial Analysts Journal*, 52(3), 71-76.

Graham et al. (2015): A Unified Model of Political Risk. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2533701 (26.11.2020).

Grandel, Mariene / Teixeira, Aurora AC (2012): Corruption and Multinational Companies' Entry Modes. Do Linguistic and Historical Ties Matter? In: *South African Journal of Economic and Management Sciences*, 15(3), 269-280.

Haggard, Stephan (1990): *Pathways from the Periphery: The Politics of Growth in the Newly Industrializing Countries*, Ithaca (New York): Cornell University Press.

Hellmann et al. (2000): Measuring Governance, Corruption, and State Capture: How Firms and Bureaucrats Shape the Business Environment in Transition Economies. In: *Policy Research Working Paper*, 2312, World Bank, Washington, DC.

Hellstrom, Johannes (2015): TeliaSonera accused over Azeri dealings. <https://de.reuters.com/article/teliasonera-azerbaijan-idUSL5N0YI34S20150527> (25.11.2020).

Henisz, Witold J. et al. (2010): Conflict, security, and political risk: International business in challenging times. In: *Journal of International Business Studies*, 41(5), 759-764.

Jensen, Nathan M. (2002): Economic reform, state capture, and international investment in transition economies, In: *Journal of International Development*, 14(7), 973-977.

Jensen, Nathan M. / Malesky, Edmund / Weymouth, Stephen (2014): Unbundling the Relationship between Authoritarian Legislatures and Political Risk. In: *British Journal of Political Science*, 44(3), 655-684.

Jensen, Nathan M. / Young, Daniel (2008): A Violent Future? Political Risk Insurance Markets and Violence Forecast. In: *Journal of Conflict Resolution*, 52(4), 527-547.

Leitner, Johannes / Meissner, Hannes (eds.) (2017): *State Capture, Political Risks and International Business. Cases from Black Sea Region Countries*. London: Routledge.

Leitner, Johannes (2017): Political Risk and International Business: Where they Interfere, Consequences, and Options. In: Leitner, J. / Meissner, H. (eds.) (2017): *State Capture, Political Risks and International Business. Cases from Black Sea Region Countries*. London/New York: Routledge, 26-40.

Li, Quan / Reuveny, Rafael (2003): Economic Openness, Democracy, and Income Inequality. An Empirical Analysis. In: *Comparative Political Studies*, 36(5), 575-601.

Noack, Rick (2019): Volkswagen CEO 'not aware' of Uighurs detained in China's Xinjiang, despite having a factory there. In: *The Washington Post*, 17.4.2019. <https://www.washingtonpost.com/world/2019/04/17/volkswagen-built-factory-chinas-xinjiang-where-up-million-uighurs-have-been-detained-its-ceo-says-hes-not-aware-that> (30.6.2020).

Olson, Mancur (1993): Dictatorship, Democracy, and Development. In: *The American Political Science Review*, 87(3), 567-576.

Sottilotto, Cecilia Emma (2013): Political Risk: Concepts, Definitions, Challenges. In: *School of Government Working Paper Series*, 6, 1-21.

Sottilotto, Cecilia Emma (2015): *Rethinking Political Risk: Concepts, Theories, Challenges*. London: Routledge.

Zucker-Boswell, Nancy (1999): The Law, Expectation, and Reality in the Marketplace: The Problems of and Responses to Corruption. In: *Law and Policy in International Business*, 30, 139-145.

Johannes Leitner

Management politischer Risiken für Unternehmen. Schwierig, aber möglich. Und wünschenswert.¹



Johannes Leitner
FH des BFI Wien

Abstract

Die Praxis des politischen Risikomanagements ist insbesondere im deutschsprachigen Raum nach wie vor mit Defiziten behaftet. Diese Defizite sind einerseits auf organisationaler Ebene zu finden, wie die wenig verbreitete systematischen Zugänge zum Management politischer Risiken. Aber auch auf individueller Ebene finden sich Faktoren, die zu einer verbesserungswürdigen Situation im Management politischer Risiken führen. Beides wird in diesem Beitrag dargestellt, um mit einem systematischen Überblick und einer Schrittfolge sowie strategischen Optionen für politisches Risikomanagement zu enden.

Political risk management in German-speaking countries such as Germany, Austria, and Switzerland is still deficient. On the one hand, these deficits can be found on the organizational level with a lack of systematic approaches to the management of political risks. On the other hand, also the individual level is a source of deficiencies, which lead to a situation in political risk management which needs to be improved. This paper portrays both aspects, and will also provide a systematic overview as well as a step-by-step roadmap and strategic options for political risk management.

1 Vorbehalte zum Management politischer Risiken

Es scheint paradox. In informellen Gesprächen mit Managerinnen und Managern international tätiger Unternehmen werden Diskussionen zu politischen Risiken und dem Managen dieser Risiken mit großem Engagement geführt. Dass der politische Kontext für unternehmerische Aktivitäten eine wesentliche Rolle spielt und dass der politische Kontext sowohl strategisch als auch operativ gemanagt werden muss, bedarf keiner weiteren Begründung. Erfahrungen und Erlebnisse werden ausgetauscht, bittere Enttäuschungen und waghalsige Entscheidungen, die aus einem „Bauchgefühl“ heraus getroffen wurden, sind zentrale Aspekte der Gespräche.

Sobald allerdings die Gesprächssituation einen offiziellen Charakter annimmt, etwa im Rahmen eines Forschungsinterviews, verschließt schon allein die Erwähnung des Wortes „politisch“ und dann noch dazu in Kombination mit „Risiko“ die Türen. Abschirmen und Abriegeln sind angesagt. Ein seriöses, tiefgründiges und wahrheitsgetreues Gespräch zu politischen Risiken und dazu,

¹ Dieses Working Paper entstand im Rahmen des Forschungsprojekts STRATOS, das durch die MA 23 der Stadt Wien finanziell gefördert wird.

Gefördert von



Stadt
Wien

Wirtschaft, Arbeit
und Statistik

wie ein Unternehmen diese im Aus- oder auch Inland managt, ist damit in vielen Fällen nicht mehr möglich. Stattdessen erschöpfen sich derartige Konversationen in allgemeinen Floskeln, deren zugespitzte Aussage jeweils ist: „Mit Politik beschäftigen wir uns nicht. Wir fokussieren auf den Markt. Im Übrigen halten sich unsere Managerinnen und Manager an die strengen internen Compliance und Corporate Governance Vorschriften.“ Diese Compliance Regeln werden dann mehr oder weniger ausführlich dargelegt, je nachdem, wie ausdifferenziert die Systeme des jeweiligen Unternehmens sind.

Immerhin, in manchen Gesprächen wird auf frühere Erfahrungen verwiesen, als man – überwiegend in Osteuropa – negative Erfahrungen mit Korruption, Bestechung und Seilschaften machte und daher bestimmte Märkte nun meide.

Aus unseren Untersuchungen der letzten Jahre wissen wir, dass Unternehmen selbstverständlich den politischen Kontext managen, ja managen müssen, um erfolgreich zu sein, und wir wissen auch, dass Unternehmen Methoden und Instrumente anwenden, um die politischen Risiken zu managen, wobei hier Unternehmen in Österreich noch wesentlich professioneller agieren könnten. (Leitner/Meissner 2020b, 2020a)

Um sich der Thematik einigermaßen seriös annähern zu können und um ein völlig artifizielles Bild der unternehmerischen Praxis zu vermeiden, sind lange bestehende Vertrauensbeziehungen und umfangreiche Kenntnisse der politischen Risikoliteratur notwendig. Ersteres, um genauere Einblicke in Unternehmen zu erhalten, Letzteres, um diese Einblicke auch systematisieren und einordnen zu können.

Dieser Beitrag will die Diskussion zum Management politischer Risiken nüchtern betrachten, indem sowohl ein Prozess als auch unterschiedliche Methoden vorgestellt werden, die zu einer besseren Entscheidung bei der Analyse und beim Management politischer Risiken führen.

2 Aufarbeiten eines Grundproblems: Veraltete Konzepte und Vorstellungen

Das Verständnis von politischen Risiken ist ein sehr traditionelles. Trotz aller Umwälzungen der geo-politischen und ökonomischen Rahmenbedingungen der vergangenen 30 Jahre reduzieren Unternehmen politische Risiken vielfach auf Enteignungen oder staatliche Interventionen, wie wir sie aus den 1970er Jahren kennen. Damals, zu Beginn der Forschung zu politischen Risiken, waren erstmals vor allem nordamerikanische Unternehmen durch die politischen Umbrüche in vielen südamerikanischen Staaten von Enteignungen betroffen. Dieses Bild dominiert nach wie vor in den Köpfen. Und das, obwohl die Konzepte und Modelle seit Jahrzehnten weiterentwickelt wurden.

Die Historie der Forschung zu politischen Risiken ist ebenso wenig linear verlaufen, wie die Geschichte selbst. Rückblickend zeigt sich, dass die jeweils aktuellen und meistdiskutierten

Definitionen von politischen Risiken eine Deutung der politischen Realitäten waren. So ist es nicht verwunderlich, dass der wissenschaftliche Diskurs zu politischen Risiken wenig Kontinuitäten aufweist, bis auf die eine Tatsache, der Kritik an einer fehlenden, umfassenden Definition von politischem Risiko.

Bereits in den 1970er Jahren hat Kobrin (1979) auf das Problem hingewiesen, dass kein klarer Rahmen für die Forschung zu politischen Risiken besteht, wodurch auch die Forschungsergebnisse unterschiedlicher Studien und Untersuchungen kaum vergleichbar seien, da jede Autorin und jeder Autor ein anderes Verständnis als Bezugsrahmen heranzieht. An dieser Kritik hat sich über Jahrzehnte wenig geändert. (Fitzpatrick 1983; Leitner/Meissner 2017; Sottilotta 2017)

Einen aufschlussreichen Einblick erlaubt die Arbeit von Sottilotta (2017), die den historischen Kontext in ihrem Literaturüberblick zu Definitionen von politischem Risiko berücksichtigt. So zeigt sich, dass der Fokus in der Forschung der 1970er Jahre auf Enteignungen von Unternehmen im Zuge sozialistischer Revolutionen lag, in den 1980er Jahren rückte das Verschuldungsproblem von Staaten in das Zentrum der Forschung und die 1990er Jahre wiederum zeigten vermehrt geopolitische Risiken wie Terrorismus im Kern der Analysen. In den 2000er Jahren zeigte sich die Forschung zunehmend selbstreflexiv, indem sie die eigenen, sehr westlich geprägten Konzepte politischer Risiken kritisiert und auch Europa und Nordamerika in die politische Risikoanalyse integrierte. Genau diese Flexibilität wurde als Vorteil der Forschung gesehen, wodurch politische Risikokonzepte immer wieder an die neuen weltweiten politischen Dynamiken und Trends angepasst werden konnten. (Jarvis 2008)

Auch die Modelle zur Analyse von Faktoren, die zu politischen Risiken führen, haben sich stark ausdifferenziert und eine permanente Entwicklung durchlaufen. Waren die ersten Modelle noch darauf beschränkt, möglichst exakte Listen von Risikofaktoren zu liefern (Miller 1992, 1993), integrierte die nachfolgende Generation an Modellen auch den institutionellen Kontext. (Alon/Martin 1998; Simon 1982) Die jüngsten Modelle versuchen zunehmend, die Risikokonstellationen unterschiedlicher Regimetyptologien besser zu verstehen und deren Auswirkungen auf unternehmerisches Handeln zu modellieren. (Jensen et al. 2013; Leitner/Meissner 2017, 2018a)

Welchen Einfluss haben etwa pseudodemokratische Systeme auf Multinationale Unternehmen (MNU)? Eine der wohl umstrittensten Fragen in diesem Forschungsstrang ist jene, ob autoritäre oder demokratische politische Systeme mit geringeren politischen Risiken einhergehen. Wäre Ersteres der Fall, dürften die USA oder auch die EU kaum führend sein bei der Anwerbung von internationalen Investoren und der Gründung von Unternehmen. Wäre Zweiteres der Fall, dann kann schwer der rasante ökonomische Aufstieg Chinas der vergangenen 20 Jahre erklärt werden, der trotz oder aufgrund eines kommunistischen, autokratischen Systems erfolgt. Ebenso wird man in jedem Land, in jedem politischen System dieser Erde MNU finden, die bereit sind, ihre Produkte und Services gewinnbringend zu verkaufen. Die Frage nach der Regimetyptologie ist demnach zu kurz gegriffen. Vielmehr sind die relevanten Faktoren in Transparenz, Rechtssicherheit, Prognostizierbarkeit und Stabilität zu suchen. (Jensen et al. 2013; Sottilotta

2017) Ebenso klar ist auch, dass nicht nur die unternehmensexternen Faktoren wie die eben beschriebenen Rahmenbedingungen eine Rolle in der politischen Risikobewertung spielen, sondern auch die Akteure in den Unternehmen selbst (Giambona et al. 2017; Maitland/Sammarino 2015) sowie die unternehmerischen Lernerfahrungen im Umgang mit komplexeren Märkten. (Johanson/Vahlne 1977; Clarke/Liesch 2017)

Trotz aller unterschiedlichen Schwerpunktsetzungen in der Forschung zum Management politischer Risiken und der damit einhergehenden Schwemme an verschiedenen Definitionen ist festzustellen, dass einige Kriterien im Kern einer jeden Definition über die Jahrzehnte relativ stabil vorhanden sind (Leitner 2017; Leitner/Meissner 2017):

Definitionen zu politischem Risiko beziehen sich stets auf den (i) Internationalen Kontext, also auf die Auslandstätigkeiten eines Unternehmens. (ii) Im Interesse stehen immer Handlungen des öffentlichen Sektors, weil der den politischen Kontext bildet. (iii) Diese Handlungen wirken auf die Geschäftstätigkeiten eines privaten Akteurs, also eines internationalen Unternehmens, das in diesem Markt aktiv ist. Und (iv) werden in der Regel die negativen Konsequenzen betrachtet, wenn etwa ein neues Gesetz verabschiedet wird, das auf die Profitabilität des Unternehmens negativ wirkt.

Politische Risikofaktoren können demnach sowohl globaler Terrorismus, Krieg oder Sanktionen darstellen, wie auch lokal ausgeprägte Korruption, politische Instabilität oder unklare Rechtslagen.

3 Verzerrungen im Management politischer Risiken

Wir haben in unseren Forschungen der vergangenen Jahre im Rahmen unseres STRATOS² Projekts gesehen, dass vor allem im Vergleich mit angloamerikanischen Unternehmen das systematische Management politischer Risiken defizitär ausfällt. (Leitner/Meissner 2018b, 2020a, 2020b) Oftmals sind die Gründe dafür in drei Bereichen zu finden: **Kognitiver Bias**, **interesseninduzierter Bias** und **Omnipotenzfantasien**. Diese Verzerrungen beeinflussen letztlich auch das operative Ergebnis eines Unternehmens, weil durch eine mangelhafte Analyse einer politischen Risikokonstellation unscharfe oder gänzlich falsche Schlussfolgerungen gezogen und Konsequenzen realisiert werden.

Der erste Problembereich liegt in einer verzerrten Informationslage durch den Interessenbias. Sind auf Headquarter-Ebene strategische Unternehmensentscheidungen zu einem Auslandsmarkt zu treffen, muss in einem ersten Schritt die einer Entscheidung zugrundeliegende Information beschafft und aufgearbeitet werden. Dabei vertrauen die Managerinnen und Manager ihren eigenen Mitarbeiterinnen und Mitarbeitern, die in dem Auslandsmarkt arbeiten, und befassen

² <https://ccbsr.fh-vie.ac.at/stratos/>

diese mit der Informationsbeschaffung. Diejenigen im Unternehmen, die an der „Front“ arbeiten, die also im Markt bei den Kunden sind, sollten auch die besten Informationen zu den politischen, ökonomischen und unternehmerischen Entwicklungen des Marktes gesammelt haben. Diese sind also die Informationsbeschaffer. Genau darin besteht eine erste Gefahr: Sales Leute werden dafür bezahlt zu verkaufen. Auch ihre Kontakte in dem Auslandsmarkt, und seien sie noch so zentral in den politischen Macht- und Entscheidungsstrukturen verankert, sind an Geschäftsmöglichkeiten ausgerichtet. Die politischen Repräsentanten haben wohl die Aufgabe, ihr Land bestmöglich darzustellen, als attraktiven Investitionsstandort zu preisen und Unternehmen davon zu überzeugen, vor Ort zu investieren. Beide Partner, sowohl der Sales Manager bzw. die Sales Managerin als auch die zentralen Repräsentanten eines Landes haben also eine inhärente Neigung, politische Szenarien zu beschönigen, zu kalmieren und schlichtweg das in den Vordergrund zu rücken, was besser funktioniert.

Ein gutes Beispiel dieser Inszenierungen sind – bei aller Wertschätzung der Bedeutung und Wichtigkeit derartiger Veranstaltungen – die länderspezifischen Events der Wirtschaftskammer Österreich. Hochrangige Vertreter eines Landes preisen selbstverständlich die großartigen Chancen und Absatzmöglichkeiten für internationale Unternehmen in ihrem jeweiligen Markt an.

Jedenfalls ist bereits die Informationsbeschaffung mit Verzerrungen versehen, sodass risikobehaftete Themen entweder abgeschwächt oder gar nicht in die weitere Analyse Eingang finden.

In dem folgenden Schritt der Analyse der vorliegenden Informationen können dann selbst methodisch korrekt angewendete Instrumente wenig zur Aufklärung beitragen, wenn die zugrundeliegenden Informationen verzerrt sind. Selbst wenn die Wahrscheinlichkeiten und Auswirkungen unterschiedlicher Risikokonstellationen ohne weiteren Bias evaluiert werden, wird das Ergebnis ein falsches sein.

Jedoch wird auch in dem Schritt der Evaluierung mit kognitiven Verzerrungen zu rechnen sein. Chancen werden überbewertet, Risiken negiert oder als wenig relevant dargestellt. Somit wird der weitere Weg versperrt, angemessene Strategien zu entwickeln, um die Risikokonstellation zu managen.

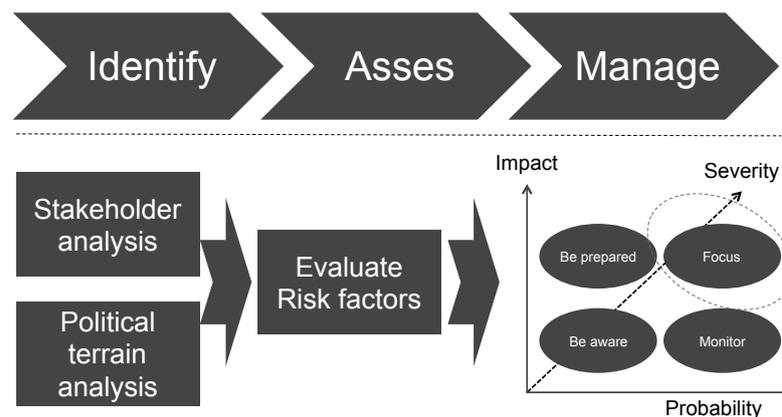
Managerinnen und Manager, die in der Verantwortung für bestimmte Auslandsmärkte stehen, können üblicherweise einen Track Record vorweisen, dass sie selbst Erfahrung gesammelt haben und daher die Risikokonstellation bestmöglich einzuschätzen in der Lage sind. Diese Ansicht ist legitim und notwendig, allerdings wird es dann toxisch, wenn die eigenen Grenzen übersehen werden. In unseren Fokusgruppen hat sich gezeigt, dass diejenigen Managerinnen und Manager, die ein profundes Verständnis über die komplexen Risikokonstellationen eines Marktes haben, auch eher der Ansicht waren, dass zusätzliche, externe Expertise eine notwendige Unterstützung darstellt (Leitner/Meissner 2018b). Zusammengefasst bedeutet das, die Personen mit mehr Einblick und Wissen über ein Thema waren sich auch viel eher der eigenen Grenzen bewusst.

Die Reflexion und das Erkennen der eigenen Defizite ist der Schlüssel zum Erfolg. Wenn ich weiß, dass ich nichts weiß, weiß ich mehr, als diejenigen, die glauben, alles zu wissen.

4 Priorisierungsprozess im Management politischer Risiken

Der Prozess im Management politischer Risiken ist im Wesentlichen in drei Schritte unterteilt, wie in Grafik 1 veranschaulicht. Im ersten Schritt gilt es, den Unternehmenskontext zu screenen, um potenzielle politische Risikofaktoren zu identifizieren. Dieser sehr bedeutende Schritt wiederum muss auf zwei Bereiche fokussieren, die durchaus miteinander in Verbindung stehen können, aber nicht müssen. Zum einen muss das politische und institutionelle Umfeld eines Marktes genau betrachtet werden. Welche politischen Dynamiken könnten auf das Unternehmen Auswirkungen haben? Wie ist die politische Stabilität in dem Markt? Welche sozialen Themen werden in der breiten Öffentlichkeit diskutiert, und könnte das auf das Projekt oder Unternehmen Rückwirkungen erzeugen, etwa durch Proteste, PR-Kampagnen oder ähnliches?

Grafik 1: Schritte im Management politischer Risiken



Quelle: McKellar 2010

Der zweite Bereich, der von großer Bedeutung sein kann, ist, ein genaues Verständnis über die Stakeholder in dem Markt zu haben. Welche Interessengruppen stehen uns positiv, welche negativ gegenüber? Muss man mit oligarchischen Strukturen rechnen, deren Interessen man nicht verletzen darf? Wer sind die Entscheidungsträger in dem Land? Die offiziellen Politiker oder mögliche Funktionäre im Hintergrund? Ebenso wie bei der Identifikation möglicher politischer Risikofaktoren im politischen Kontext muss auch die Stakeholderanalyse ein Bild entwerfen, das zur Identifikation möglicher riskanter Konstellation beiträgt.

Sind die potenziellen Risiken identifiziert, muss in einem zweiten Schritt eine Analyse oder auch Evaluierung dieser Faktoren erfolgen. Wie in der Risikobewertung üblich, werden zwei Dimensionen eines jeden Faktors in Betracht gezogen. Zum einen muss soweit möglich eine Bewertung der Eintrittswahrscheinlichkeit erfolgen. Diese Bewertung ist gerade bei politischen

Risiken mit großen Schwierigkeiten verbunden, weil oftmals keine historischen Beobachtungen zur Verfügung stehen, die als Grundlage der Beurteilung herangezogen werden können. Revolutionen, politische Krisen, Machtwechsel oder auch Korruption sind sehr schwer oder kaum quantifizierbare Faktoren. (Rice/Zegart 2018) Hier bedarf es der qualitativen Zugänge, um die zugrundeliegenden Kausalitäten zu verstehen und daraus abgeleitete Konsequenzen beurteilen zu können. Gleichzeitig neigen Menschen dazu, seltene Ereignisse in ihrer Eintrittswahrscheinlichkeit zu unterschätzen. (Bremmer/Keat 2009)

Neben der Wahrscheinlichkeit, ob ein bestimmtes Risiko sich materialisiert, muss auch beurteilt werden, welche Auswirkung der Risikofaktor auf das Unternehmen hat. Nehmen wir als Beispiel Usbekistan unter der Herrschaft des ehemaligen Präsidenten Islom Karimov, der bis 2016 das Land autokratisch regierte und auch weitestgehend international isolierte. Als ausländisches Unternehmen musste man bestmögliche Verbindungen zum Präsidenten unterhalten, vor allem, wenn große staatliche Aufträge im Spiel waren. Für Unternehmen besteht das Risiko eines ungeplanten Machttransfers vor allem in der Disruption bekannter Machtstrukturen. Etablieren sich plötzlich neue Machtzentren, die auch die Entscheidungshoheit über die Ressourcenallokation haben, müssen möglicherweise erst neue Netzwerke erschlossen werden. Sind Konkurrenzunternehmen schneller, gehen womöglich Aufträge verloren. Die Auswirkung könnte also durchaus eine große Bedeutung für das Unternehmen haben.

Sind schließlich alle in Schritt 1 identifizierten Risikofaktoren bewertet, kann im Schritt 3 eine Priorisierung vorgenommen werden. Hier besteht die Aufgabe darin, auf diejenigen Risikofaktoren zu fokussieren, die eine relativ hohe Eintrittswahrscheinlichkeit haben und auch in ihren Auswirkungen wesentlich sind. Anhand der beiden Dimensionen Wahrscheinlichkeit und Auswirkungen kann eine Matrix aufgespannt werden, die eine Einordnung der einzelnen Risikofaktoren ermöglicht. Diese Matrix erlaubt auch eine schnelle optische Darstellung, welche Faktoren prioritär gemanagt werden müssen. Wir sehen in Grafik 1 in der Matrix den Bereich im nordöstlichen Quadranten, in dem wir die zu priorisierenden Risiken finden. Im südöstlichen Quadranten wiederum sind jene Faktoren, die zwar für sich keine besonderen Auswirkungen, aber eine hohe Eintrittswahrscheinlichkeit haben. Diese müssen unter Beobachtung bleiben, denn bei sehr häufig hintereinander eintretenden Fällen können sich auch die einzelnen Auswirkungen addieren und so für das Unternehmen problematisch werden. Etwa, wenn permanent ungerechtfertigte, politisch motivierte Steuerprüfungen durchgeführt werden, ist der Einzelfall kein Problem, wenn das aber innerhalb weniger Monate immer wieder stattfindet und das ganze Unternehmen deshalb stillsteht, summiert sich die Auswirkung zu einem schwerwiegenden Problem. Im südwestlichen Quadranten sind die Faktoren zu finden, die sowohl eine geringe Wahrscheinlichkeit als auch geringe Auswirkungen haben, insofern müssen diese nicht weiter beachtet werden. Im nordwestlichen Quadranten schließlich finden sich diejenigen Faktoren, die zwar eine sehr geringe Eintrittswahrscheinlichkeit haben, aber in ihren Auswirkungen fatal sein können. Für diese Faktoren muss ein Unternehmen Szenarien haben, was im Eintrittsfall geschehen muss, damit die Firma nicht Schaden nimmt.

5 Strategien im Management politischer Risiken

Unternehmen stehen beim Managen der politischen Risiken im Wesentlichen vier Strategien zur Verfügung, die von der Akzeptanz bis zur Vermeidung reichen, wie in Tabelle 1 dargestellt.

Tabelle 1: Strategien zum Managen politischer Risiken.

Generic Strategies	Refined	Examples
Accept	You simply accept the risk and do not take any action	Start the business and hope for the best
Mitigate	You try to reduce either the probability or the impact of the risk	<ul style="list-style-type: none"> • Political strategies • Stakeholder Mgmt • Portfolio Mgmt • Intelligence
Transfer	You transfer the risks to other partners who are willing to bear them	<ul style="list-style-type: none"> • Insurance • Outsourcing risky actions • Brokers • Decoupling
Avoid	You do not take actions that inherently are associated with certain risks	<ul style="list-style-type: none"> • You do not pursue a business opportunity

Quelle: Eigene Darstellung.

Die **Akzeptanzstrategie** bedeutet nicht mehr, als dass ein Unternehmen die mit einer Geschäftstätigkeit einhergehenden politischen Risiken kennt, aber so wie sie sind akzeptiert, ohne weitere Maßnahmen zu treffen. Diese Strategie ist legitim und wird auch im täglichen Leben permanent angewendet, andernfalls wären wir handlungsunfähig. Wichtig aber ist, dass diese Strategie nur dann auch erfolgversprechend ist, wenn zugrundeliegenden Risiken tatsächlich bekannt sind und korrekt bewertet wurden. Wenn Risiken aus Ignoranz oder Unwissenheit akzeptiert werden, werden die negativen Konsequenzen umso wahrscheinlicher eintreffen.

Mitigierungsstrategien zielen darauf ab, entweder die Eintrittswahrscheinlichkeit und/oder die Auswirkungen eines politischen Risikos abzuschwächen oder gänzlich zu verhindern. Das kann etwa durch die Anpassung der Markteintrittsstrategie (Jimenez 2010; Jimenez et al. 2014; Alcantara/Mitsuhashi 2013) erfolgen, oder aber auch durch politische Strategien (Hillman et al. 1999), durch ein aktives Stakeholder Management oder andere risikoreduzierende Aktivitäten. Eine weitere Option besteht darin, die Risiken an Dritte zu **transferieren**, die gegen eine monetäre Leistung die Risiken übernehmen. Als Beispiel dienen sämtliche Versicherungen, die gegen eine Gebühr bestimmte Risiken übernehmen. Im Falle von politischen Risiken finden sich oft staatsnahe Einrichtungen zur Absicherung und Förderung von Exporten, wie die Österreichische Kontrollbank (ÖKB), aber auch private Anbieter übernehmen politische Risiken. Es können jedoch auch riskante Aktivitäten an externe Akteure ausgelagert werden, um das Unternehmen

möglichst von dem Risiko zu entkoppeln, etwa wenn Geschäftstätigkeiten in sehr korrupten Märkten an lokale Einrichtungen ausgelagert werden. Schließlich kann ein Unternehmen aber immer zu der Entscheidung kommen, dass die politischen Risiken zu hoch sind und daher die Geschäftstätigkeit vermieden wird, also eine **Vermeidungsstrategie** realisiert wird.

6 Der schlimmste Fehler: Augen zu und hoffen auf das Beste

Das Bauchgefühl kann ein guter Ratgeber sein. Allerdings hängt die Qualität des Bauchgefühls im Kontext politischer Risiken – nicht nur, aber auch – ganz wesentlich von der Qualität des Erfahrungslernens eines Managers oder einer Managerin ab. (Maitland/Sammartino 2015) Die Qualität des Erfahrungslernens macht einen entscheidenden Unterschied aus. Allein die Präsenz – wenn auch langjährig – in einem Auslandsmarkt zeigt wenig Einfluss auf die Qualität des Bauchgefühls. Es sind Aufgaben wie langjährige Leitungsfunktionen mehrerer ausländischer Tochtergesellschaften, Senior Level Positionen als CEO oder Board Member, die dazu führen, innere Landkarten zu erstellen, die vor allem die kausalen Beziehungen unterschiedlicher Ereignisse erklären können und die Auswirkungen auf das Unternehmen abschätzen lassen können.

Dennoch ist ein systematisches Management politischer Risiken immer von Vorteil, um zwei Fehler zu vermeiden: Entweder den Fehler, ein Projekt voranzutreiben oder eine Investition zu tätigen, das bzw. die durch politische Risiken unrentabel ist. Oder aber, eine an sich profitable Entwicklung zu vermeiden, weil die Risikokonstellation zu komplex erscheint.

Für ein Unternehmen der schlimmste Fall ist aber, wenn Entscheidungen aus Ignoranz und Unwissen getroffen werden.

Literaturverzeichnis

Alcantara, Lailani Laynesa / Mitsuhashi, Hitoshi (2013): Dynamics of entering politically risky foreign markets. In: *Management Research Review*, 36(6), 580-595.

Alon, Ilan / Martin, Matthew A. (1998): A Normative Model of Macro Political Risk Assessment. In: *Multinational Business Review*, 6(2), 10-19.

Bremmer, Ian / Keat, Preston (2009): *The Fat Tail. The Power of Political Knowledge for Strategic Investing*. Oxford, New York: Oxford University Press.

Clarke, James E. / Liesch, Peter W. (2017): Wait-and-see strategy: Risk management in the internationalization process model. In: *Journal of International Business Studies*, 48(8), 923-940.

Fitzpatrick, Mark (1983): The Definition and Assessment of Political Risk in International Business: A Review of the Literature. In: *The Academy of Management Review*, 8(2), 249-254.

Giambona, Erasmo / Graham, John / Campbell, Harvey (2017): The management of political risk. In: *Journal of International Business Studies*, 48(4), 523-533.

Hillman, Amy J. / Zardkoohi, Asghar / Bierman, Leonard (1999): Corporate political strategies and firm performance: Indications of firm-specific benefits from personal service in the U.S. government. In: *Strategic Management Journal*, 20(1), 67. <http://search.proquest.com/docview/225007813?accountid=2910>

Jarvis, Darryl S. L. (2008): Conceptualizing, analyzing and measuring political risk: The evolution of theory and method. Lee Kuan Yew School of Public Policy Research. Singapore (Research Paper, LKYSP08-004).

Jensen, Nathan M. / Malesky, Edmund / Weymouth, Stephen (2014): Unbundling the Relationship between Authoritarian Legislatures and Political Risk. In: *British Journal of Political Science*, 44(3), 655-684.

Jimenez, Alfredo (2010): Does political risk affect the scope of the expansion abroad? Evidence from Spanish MNEs. In: *International Business Review*, 19(6), 619-633.

Jimenez, Alfredo / Luis-Rico, Isabel / Benito-Osorio, Diana (2014): The influence of political risk on the scope of internationalization of regulated companies: Insights from a Spanish sample. In: *Journal of World Business*, 49(3), 301-311.

Johanson, Jan / Vahlne, Jan-Erik (1977): The Internationalization Process of the Firm - A model of knowledge development and increasing foreign market commitments. In: *Journal of International Business Studies*, 8(1), 23-32.

Kobrin, S. (1979): Political Risk: A Review and Reconsideration. In: *Journal of International Business Studies*, 10(1), 67-80.

Leitner, Johannes (2017): Political risk and international business: Where they interfere, consequences, and options. In: Leitner, J. / Meissner, H. (eds.): *State Capture, Political Risks and International Business. Cases from Black Sea Region Countries*. London/New York: Routledge, 26-40.

Leitner, Johannes / Meissner, Hannes (eds.) (2017): *State Capture, Political Risks and International Business. Cases from Black Sea Region Countries*. London/New York: Routledge.

Leitner, Johannes / Meissner, Hannes (2018a): Corruption in Ukraine: Soviet legacy, failed reforms and political risks. In: Warf, B. (eds.): Handbook on the Geographies of Corruption. Cheltenham: Edward Elgar, 183-195.

Leitner, Johannes / Meissner, Hannes (2018b): Politisches Risikomanagement aus der Perspektive österreichischer Managerinnen und Manager. In: FH BFI Wien (Hg.): Working Paper Series, 101. <https://www.fh-vie.ac.at/de/seite/forschung/publikationen/politisches-risikomanagement-aus-der-perspektive-oesterreichischer-managerinnen-und-manager> (2020)

Leitner, Johannes / Meissner, Hannes (2020a): Denn sie wissen nicht, was sie tun. Eine Bestandsaufnahme zum Management politischer Risiken multinationaler Unternehmen. In: Wirtschaft und Management, Bd. 28, 7-20.

Leitner, Johannes / Meissner, Hannes (2020b): Good Practices im Management politischer Risiken. Eine Analyse der Post-Unternehmen aus der DACH-Region. In: Wirtschaft und Management, Bd. 28, 21-34.

Maitland, Elizabeth / Sammartino, Andre (2015): Decision Making and Uncertainty: The Role of Heuristics and Experience in Assessing a Politically Hazardous Environment. In: Strategic Management Journal, 36(10), 1554-1578.

McKellar, Robert (2010): A short guide to Political Risk. Aldershot: Gower.

Miller, Kent D. (1992): A Framework for Integrated Risk Management in International Business. In: Journal of International Business Studies, 23(2), 311-331.

Miller, Kent D. (1993): Industry and Country Effects on Manager's Perceptions of Environmental Uncertainty. In: Journal of International Business Studies, 24(4), 693-714.

Rice, Condoleeza / Zegart, Amy B. (2018): Political Risk. How Businesses and Organizations can Anticipate Global Insecurity. New York: Twelve.

Simon, Jeffrey D. (1982): Political Risk Assessment: Past Trends and Future Prospects. In: Columbia Journal of World Business, 17(3), 62-72.

Sottillotta, Cecilia E. (2017): Rethinking Political Risk. London/New York: Routledge.

David Morris

The Huawei paradox: cyber-risks in a deteriorating geopolitical climate



David Morris
Corvinus Universität, Budapest
& United Nations Economic
and Social Commission for
Asia and the Pacific (ESCAP)

Abstract

Im sich verschlechternden geopolitischen Wettstreit zwischen den Vereinigten Staaten und China ist ein Unternehmen zum Symbol für potenzielle Risiken geworden: Huawei ist ein nationaler Spitzenkonzern im aufstrebenden Technologiesektor Chinas, wird jedoch von den USA und einigen ihrer Verbündeten als potenzieller Vektor für Cyber-Angriffe einschließlich Spionage und Sabotage gefürchtet. In einer technologisch vernetzten Welt besteht das Paradoxon darin, dass Firmen wie Huawei ohne Vertrauen und ohne internationale Zusammenarbeit diese Worst-Case-Risikoszenarien nicht widerlegen können. Die Logik des Huawei-Paradoxons bedroht die Entkopplung und provoziert die Verzweigung der Welt in zwei rivalisierende technologische Systeme, mit Auswirkungen auf die internationale Sicherheit, die internationalen Beziehungen und die internationale Wirtschaft. Eine politische Risikoanalyse und -bewertung kommt zu dem Schluss, dass die Risiken eher von geopolitischen Faktoren als von unternehmens- oder länderspezifischen Faktoren herrühren und daher (sofern der politische Wille vorhanden ist) nur auf der globalen politischen Ebene mit durchsetzbaren Regeln, Normen und Standards und auf der nationalen Regierungsebene mit Maßnahmen zur Risikovermeidung oder zum Risikomanagement und zur Risikominderung gelöst werden können.

One firm has become emblematic of risk in the deteriorating geopolitical contest between the United States and China. Huawei is a national champion of China's emerging technology sector but is feared by the US and some of its allies as a potential vector of cyber-attacks including espionage and sabotage. In a world of connected technology, the paradox is that in the absence of trust and international cooperation, firms such as Huawei cannot disprove worst-case risk scenarios. The logic of the Huawei paradox threatens decoupling and bifurcation of the world into two rival technological systems, with repercussions for international security, international relations and the international economy. A political risk analysis and assessment concludes that the risks originate from geopolitical factors rather than factors specific to the firm or country of operations and can therefore only be resolved (if there is political will) at the level of global governance with enforceable rules, norms and standards and at the level of national governance with risk avoidance or risk management and mitigation measures.

1 Introduction

The extraordinary case of Huawei, a world-leading private sector firm from China, and the United States (US) government campaign to remove the firm from global supply chains, is playing out as a critical case in the deteriorating geopolitical contest between the two major powers. The trajectory of the Huawei story remains uncertain at the time of writing, but it raises a paradox that warrants further investigation – that, in an absence of trust and international cooperation,

firms such as Huawei cannot disprove fears of worst-case scenarios of malicious cyber activity. The logic of this paradox leads to the inevitable debate, currently underway, about decoupling between China and the US and bifurcation of the world into two rival technological systems. Accepting the limitations of analysing a contemporary case – with results yet to be seen – this paper applies a political risk framework in seeking to understand the issues and their implications for governments, firms and communities.

After four decades of economic modernisation, China's economy is transitioning from a high-growth phase of low-cost manufacturing and capital investment to a new phase of demand-driven, higher value production, seeking to avoid the so-called middle-income trap. The vibrant private sector-dominated southern city of Shenzhen, a traditional base for economic reform and opening, has become a hub for technological innovation and is home to tech innovators such as Tencent, DJI, ZTE and Huawei. The government's so-called "Made in 2025" strategy to become more self-reliant and a globally competitive leader in new technologies, including mobile telecommunications, artificial intelligence and quantum computing, has been met with alarm in the US and Europe, which have traditionally enjoyed technological dominance (Zenglein/Holzmann 2019). In recent years, as US President Trump launched a trade war with China, accusations were commonly levelled that Chinese firms were engaging in cyber-espionage and hacking to steal corporate secrets (RWR Advisory Group 2019). The risks became heightened as new high-speed connectivity and transportation capabilities of Fifth Generation (5G) communications networks promised in the near future to transform the application of big data and artificial intelligence, joining up not only information but an "internet of things" driving devices such as autonomous vehicles and even weapons.

Huawei Technologies Co. Ltd., one of China's leading telecommunications firms and a global leader in 5G, has been singled out in recent years, as both a competitive threat to other industry players and as a claimed cyber-security risk. The firm is certainly a major competitive threat to the US aspirations to maintain technological dominance. Over decades, Huawei invested in a massive research and development effort to achieve its market-leading position. Like other globalised Chinese firms, it became deeply embedded in international supply chains, partnering with firms and governments around the world, developing national broadband infrastructure and other communications network and consumer products and services.

Huawei has long been considered a national security risk by the security establishment of the US and some of its allies because of the military background of its founder, Ren Zhengfei, and other staff links to state security services (Balding 2019), although no evidence has been presented publicly of widely-repeated claims that Huawei has facilitated espionage. In turn, Huawei has consistently denied the claims.

In August 2018, Australia became the first country to effectively ban Huawei from supplying a 5G network on national security grounds, after previously excluding Huawei from developing its national broadband network and from laying a broadband cable between Australia, Solomon

Islands and Papua New Guinea. The decision attracted international attention, because Australia had for many years been one of the most economically integrated G20 economies with China, enjoying a massive trade surplus, while at the same time being a staunch US ally. The decision was reportedly based on an intelligence assessment that Chinese firms could theoretically be required by the Chinese government to compromise Australia's 5G network (Hartcher 2018; Hunter 2019; McKenzie/Galloway 2020) and that Australia was incapable of mitigating risks of implanted network coding or equipment backdoors that could threaten critical infrastructure (Bryan-Low et al 2019; McKenzie/Galloway 2020). The head of the Australian Signals Directorate's signal intelligence and offensive cyber missions, Simeon Gilding, noted trust had been eroded by recurrent Chinese hacking of foreign networks, including in Australia (Gilding 2020).

Following the Australian decision, the US administration stepped up its campaign against Huawei. In May 2019, the US Commerce Department placed Huawei on a trade blacklist, including restricting access to US components, citing national security concerns (Lim/Ferguson 2019). Despite Huawei's 5G leadership, the US move demonstrated its asymmetric market power because of its continued technological superiority in advanced semi-conductors and computer chips, on which firms such as Huawei depend (Fernandes 2019). The move forced Huawei to replace US-sourced components, which it had initially achieved by the end of 2019 by sourcing components from non-US suppliers, but its inability to license popular US applications such as those previously sourced from Google caused a fall in Huawei mobile phone sales in Western markets (Whalen/Fifield 2019).

In a dramatic episode in December 2018, the US requested Canada to arrest and detain Huawei's Chief Financial Officer, Meng Wanzhou, while she transited Vancouver airport, travelling between Hong Kong and Mexico. The US sought her extradition for fraud, charging that Meng covered up attempts by Huawei entities to evade US sanctions against Iran. The personalised action against Meng (who happened to be founder Ren's daughter) suggested an element of geopolitical theatre. Targeting a senior executive is a highly unusual action and, indeed, numerous US and other international firms have been pursued for violating US sanctions against Iran but senior executives have not typically been arrested or taken into custody (Sachs 2018). The drama continued with China detaining two Canadians, Michael Kovrig and Michael Spavor, on spying charges, in what appeared to be alarming tit-for-tat punishment of Canada. Further, in 2019, Huawei was charged by the US with stealing intellectual property (Department of Justice 2019).

The campaign continued in phases to pressure Huawei, while escalating a tense geopolitical confrontation with China. In early 2020, the US government provided US\$1 billion for telecommunications carriers to "rip and replace" Huawei and ZTE equipment from US networks (Heater 2020). In May 2020 the US Department of Commerce introduced new requirements for foreign chip makers that use US technology to apply for a licence to sell chips to Huawei, then a few months later closed that loophole altogether, in a further squeezing of Huawei's supplies of advanced semiconductors (Li/Cheng/Yu 2020; Department of Commerce 2020).

Then the Trump administration's economic coercion was matched with a new ideological "clean" versus "dirty" narrative. In August 2020, the US government unveiled its so-called "Clean Network", an alliance of "trusted" countries and firms committed to removing "authoritarian malign actors, such as the Chinese Communist Party" from their cyber supply chains (Department of State 2020). It was accompanied by a range of measures securitising tech supply chains such as increased investment in strategic research and development to compete with China, a fund for re-shoring semiconductor manufacturing to the US and a \$60 billion International Development and Finance Corporation to encourage developing countries not to buy from Chinese suppliers (Capri 2020). Moves were even made by the Trump administration to ban popular Chinese app WeChat and to force the sale of another popular app TikTok to a US company, although at the time of writing it was unclear of the outcome.

Despite the US campaign against Huawei, the firm nevertheless continues – at the time of writing – to be an attractive partner to a wide range of governments, firms and consumers across much of the world because of its technological leadership and cost competitiveness. Huawei has partnerships with more than fifty international carriers to provide 5G network equipment and services (Pham 2019). In the advanced market of Europe, there is a highly competitive environment between Huawei, which is recognised as the leader in 5G network technology and the lowest cost supplier, and Ericsson, which is considered by many in the industry to provide higher quality. Huawei has won contracts to supply half of the 5G network in Germany and Spain, while on the other hand Ericsson has won contracts in Norway and Hungary (Fletcher 2019).

Both Germany and the United Kingdom (UK) planned to proceed with Huawei for non-core components of their 5G networks despite confidential US security briefings (Ikenson 2019; Perez 2019; Mikhailova 2020), although after the US extended its sanctions on Huawei the UK announced it would delay its 5G rollout and phase out all Huawei equipment by 2027 (Dowden 2020). UK intelligence agencies have scrutinised Huawei, which allows full examination of its hardware and software products by local security experts at a jointly-managed cybersecurity evaluation centre. While the centre reported technical issues of concern in Huawei's engineering processes, it did not believe these were the result of Chinese state interference (Soo/Zhang 2020).

In the developing world, no countries have been willing – so far – to give up the option of utilising Huawei, despite US pressure, although India is expected to do so. Huawei has been a longstanding provider of wireless networks (from 3G to 4G) and other services and products from countries in the Asia Pacific region to Africa (Gu 2019). Huawei has also been a key actor in China's so-called "digital silk road" partnerships utilising concessional finance to aid developing countries in building satellite, underwater and terrestrial communications networks and so-called "safe cities" utilising artificial intelligence technology for facial recognition. While the latter projects are ostensibly aimed at improving public safety and crime detection, such as in Huawei's home city of Shenzhen where authorities claim more than one million surveillance cameras have helped solve 80 percent of criminal cases (Zheng, 2019), these programs have also been accused of

exporting the Chinese “surveillance state” model (Dirks/Cook 2019; Hillman/McCalpin 2019). Critics point to risks that Huawei and its Chinese partner firms are establishing infrastructure that could provide the Chinese government access to data from foreign countries, extending Chinese governance models and enabling authoritarian surveillance and social control (Polyakova 2019). Huawei has even been accused of providing intercepted data to African governments to spy on, locate and silence political opponents (McMaster 2020).

2 Methodology

A political risk framework is utilised in the discussion below, including (as recommended by Sottolotta 2017): risk identification, risk analysis, risk assessment and, finally, an outline of risk management approaches. Political risk is traditionally understood in international business literature to be concerned with comprehending, forecasting and responding to “macro” and “micro” non-economic discontinuities, such as socio-political, cultural or other factors in the external environment that impact on international actors (Robock 1971). Macro factors are commonly identified at the country level, sometimes described as the “catalogue school” (Jarvis 2008), because such an approach tends to generate a list of salient factors in the national governance environment that generate risks, from policy instability to corruption and law and order issues. Micro factors are usually understood to be those that are generated by a particular firm or a particular project (Alon/Herbert 2009). In all cases, a risk indicates a likelihood of an event or process that can be identified, understood and managed or mitigated (Fägersten 2015), even if there will always be uncertainty about factors that can inevitably be perceived subjectively (Kobrin 1979).

There is a further category of political risk that is expected to be relevant to this case: geopolitical risk. This is a term traditionally applied to measurable conflicts or other events or processes disrupting international peace and security such as, for example, Russia’s hybrid warfare tactics in Ukraine or the destruction caused by international terrorism (Wernick 2006). More particularly for this discussion, geopolitical risk has also been understood as describing the effects of major power competition, but it has usually been represented in positivist, zero-sum surveys of “objective” factors such as competition for resources, ports and industrial regions (Sykulski 2014). Whether the US campaign against Huawei can be reduced to a zero-sum attempt to squeeze out a geopolitical rival, or whether it raises more complex questions including technological security, remains an unanswered question. The claimed risks, however, certainly arise because of the geopolitical contest between the US and China.

Political (or geopolitical) risk can be assessed quantitatively and qualitatively. International financial institutions, political risk advisory firms and scholars (such as Alon/Martin 1998) have developed elaborate models with weightings for each risk, and produce rankings for risk to provide general guidance for decision makers. This approach is applicable, for example, to predicting the likelihood of political instability or corruption in a particular business environment or

for estimating effects of war or terrorism. However, many political (and geopolitical) risks are processes that are more usefully investigated qualitatively (Fitzpatrick 1983). The evolving case of Huawei in the contemporary, deteriorating geopolitical climate, will be discussed here in qualitative terms. There is no consensus around the claimed risks, with competing narratives about international relations and subjective views about security, governance, economic and social implications.

3 Risk identification

3.1 Security risk/threat

The case of Huawei has become emblematic of deteriorating relations between the US (and some of its allies) and China, evoking fears of security threats embedded in national telecommunications networks connecting populations, devices and critical infrastructure. While the author has no access to US or other intelligence assessments, the claims on the public record that Huawei could be a vector for, firstly, cyber-attacks such as sabotage of critical infrastructure are very serious claims indeed. The claims indicate that, even if likely in only “worst case” scenarios of major power confrontation or conflict, a perceived cyber-attack risk exists, which could indeed constitute a security threat if actualised against strategic infrastructure or systems. Secondly, the espionage claims represent qualitatively different, although also serious, security questions. Even in “normal” conditions of geopolitical competition, without escalation to confrontation or conflict, states can be expected to engage in espionage, including cyber-espionage. Given the well-established evidence of sophisticated espionage by the US and its “Five Eyes” partners, it is highly likely that China would also utilise all available means to conduct espionage. Huawei’s widespread presence in international telecommunications networks therefore generates a reasonably-founded espionage risk although, as will be discussed below, no publicly-available evidence of such exists and the firm denies it would agree to government demands for spying. Thirdly, Huawei’s involvement in digital silk road partnerships between China and a wide range of developing country partners is claimed to generate a security risk that China will export its “surveillance state” model. Overall, the Huawei paradox raises considerable security risks.

3.2 International relations risk

The campaign against Huawei (on the basis that it is a Chinese, albeit private sector, firm) in itself potentially undermines international cooperation in developing rules, norms and standards for the digital economy. The US-led “Clean Network” seeks to decouple from Chinese supply chains and potentially divides the digital economy into at least two spheres of rules, norms and standards, just as China’s “Great Firewall” had already driven a wedge in the global internet. Weakened international cooperation will in turn undermine global governance institutions which might otherwise build and sustain rules, norms and standards to reduce cyber risks for

governments, firms and communities. Further, the demarcation of the digital economy into US-led and China-led spheres risks enhancing the foreign influence of these major powers over other states within their spheres, including not only favouring firms originating in each major power but increasing the likelihood that states may be influenced to support their major power partner on other matters from international rule-making to targeting firms (or even individuals representing firms) from third countries. Overall, the Huawei problem poses serious challenges to international relations.

3.3 Economic cooperation risk

Huawei is a stark example of the risk of economic coercion by a major power, with the US targeting a private sector firm and wielding a range of state measures to constrain the firm in international markets. In the absence of evidence on the public record of any wrongdoing (although, to be sure, potential risks), the action sets an alarming precedent for how economic coercion may be deployed by major powers against other international firms as the geopolitical climate continues to deteriorate. It increases the likelihood of counter-measures and therefore generates risks for a wide range of other international firms. The implications of the actions against Huawei transmit throughout global supply chains, with all international firms that supply Huawei impacted by US executive and legislative restrictions and liable to sanction for not conforming. As noted above, the result may ultimately be decoupled supply chains, which would generate adjustment costs as well as long term costs of duplicating and in some cases sourcing from higher cost suppliers. Firms on both sides will lose access to valuable markets. The Huawei dilemma poses serious questions about future international economic cooperation and is a risk to globalisation processes.

Identified risks

Security (threat)	International relations	Economic cooperation
Cyber-attack risk	Rules/norms risk	Coercion risk
Espionage risk	Institutional risk	Supply chain risk
Surveillance state risk	Foreign influence risk	Globalisation risk

4 Risk analysis

4.1 Security risk/threat

The central security concern rests upon a theoretical proposition that Chinese technology underpinning international communications systems could be weaponised by the Chinese state. The US and its allies, amongst others, distrust the authoritarian Chinese party state and fear its growing technological and military capabilities. Despite being a private firm, observers note Huawei could be co-opted to serve the national security objectives of the Chinese government

and forced to facilitate espionage or cyber-attacks (Gilding 2020). Article 7 of China's National Intelligence Law of 2017 is particularly cited, which requires that Chinese firms and their employees cooperate with national intelligence agencies lawfully carrying out their work (Girard 2019). The US government has equivalent powers (Eisenstein/Halpert 2018).

The risk of espionage would appear on the face of it to be realistic. After all, it is well documented, including in the Snowden and WikiLeaks revelations, that the US and its Five Eyes (Australia, Canada, United Kingdom and New Zealand) partners similarly engage in espionage (Snowden 2019), including co-opting Apple, Facebook, Google and other firms to collect data (Biddle 2020). There is no reason to believe China is not doing the same, regardless of the geopolitical climate and regardless of standard government denials. The perennial risks of espionage raise highly technical questions about capabilities of detection and protection. These are relevant questions not only in relation to Huawei, but for all telecommunications systems and the complex global supply chains for equipment and software.

The risk of cyber-sabotage is much more dependent on the state of the geopolitical climate. In a state of contest, confrontation and potential conflict, there is a risk that technically undetectable malicious code or "kill switches" are implanted into 5G networks, which could be used for cyber-attacks on critical infrastructure. Such aggressive actions might have been less likely during previous years when the US and China and other countries were cooperatively engaged in building interdependent economies. Indeed, Huawei has been intent on building its international reputation as a trusted provider of state-of-the-art technology and it would appear to be self-defeating to allow itself to be used as a platform for hostility against its customers. In the new era of geopolitical competition however, featuring new flashpoints of confrontation, economic decoupling and more aggressive positioning by both the US and China, the risks become more likely that firms such as Huawei (or indeed firms on the US side) might be co-opted or compromised for more aggressive security operations. This is not a risk specific to the firm, but a risk of hostile state action.

Looking forward, the security of 5G networks will become even more important for the connected technologies of the future. Indeed, risks will not only be generated by major power geopolitical contest but governments will also need to protect against cyber-attack from other states, terrorist organisations or rogue individuals. Whether Huawei can be enlisted as a partner in protecting against such risks, or whether it is a vector of risk, will depend upon normative perspective. Further, countries along the so-called digital silk road that are cooperating with Huawei to build "smart city" infrastructure may see more opportunities than risks, while observers from liberal democracies will be concerned about how such infrastructure might in turn be used for surveillance and social control. Whether China is exporting authoritarianism along its digital silk road rests upon the question of agency. How safe city or other programs are deployed by host governments is, at the end of the day, a matter for them rather than China (Weiss 2019). After all, US, European and Japanese firms also export facial recognition technology that could be used to

target groups or individuals but are not accused of exporting authoritarianism. This underlines the normative bias that runs through most of the narratives about Huawei.

4.2 International relations risk

The Huawei case exposes a critical gap in global governance. Inadequate rules, norms, standards and institutions exist to manage risks of globally interconnected technology. The international community is ill-prepared for the implications of the so-called “fourth industrial revolution” of big data, artificial intelligence and an internet of things, composed of connected devices and networks. The digital economy has emerged at a time of unipolarity in the international system and a weakening commitment from the US, as the dominant power, towards multilateralism. In the early stages of the digital economy, US firms such as Facebook and Google wielded significant, largely unregulated power. While the internet evolved with some private sector oversight of certain rules (such as domain names), it had no agreed set of international norms or standards and certainly no international enforcement. In the absence of rules, norms, standards and institutional enforcement, technologies generating risks have developed ahead of technical capabilities to manage those risks. Indeed, technical experts claim the complexity of telecommunications technology renders it impossible to guarantee against malicious code or backdoors in equipment (Lysne 2018; Chang 2020). Nevertheless, the risk of malicious action has not prevented the international community from developing – and abiding by – rules, norms, standards and institutions in numerous areas of strategic importance, from food safety to aviation. The lack of discussion about governance options for emerging technologies is therefore remarkable.

Governance of 5G telecommunications has become embroiled in the US-China geopolitical contest, as has governance of the internet. The US has opposed any expansion of the mandate of the International Telecommunications Union (ITU), one of the oldest international organisations, to govern digital communications. Meanwhile, China has developed a clear ambition to become the rule-setter and norm maker in internet governance and cyber sovereignty (Schia/Gjesvik 2017; Wang 2020), as well as in other transformational technologies such as blockchain and its applications in finance, manufacturing, transport, food safety and public security (Cai 2019; Stockton 2020). Across its “digital silk road” partnerships with developing nations, China has promoted uniform standards for 5G rollout (consistent with those set by the ITU), as well as for artificial intelligence and satellite navigation systems (Chan 2019). China will likely wield influence amongst its technological partners in the rules, norms and standards that will develop over time. China – together with firms such as Huawei – has been actively promoting its cyber governance model at World Internet Conferences, the ITU, the International Standardisation Organisation and the International Electrotechnical Commission and the two United Nations (UN) working groups, the Group of Governmental Experts and the Open-Ended Working Group. China can be expected to have the support of a significant number of developing countries.

While the US has begun to participate more actively in these forums in recent times, a fundamental clash of world views makes it unlikely consensus can be achieved. The Chinese government’s

aims in cyber governance include maintenance of social stability and protection from foreign influence, deemed to require control of domestic information that is perceived as a threat to the regime. Consistent with its combination of Confucian cultural roots and Marxist-Leninist political ideology, the Chinese party states rules “by law”, in contrast with the liberal Western notions, “rule of law” and contested power. China’s approach to cyber governance is therefore focused on the state’s ability to control content, which includes network security, while Western approaches are focused on network security and not content. China proposes global standards for data security, while the US is moving to establish its so-called “Clean Network” to set standards amongst a set of “trusted” partners, which appears to ignore the global interconnectedness of supply chains and in particular data, with the emergence of cloud technologies and electronic commerce that rely upon free flow of data. China and the US also take opposing positions on governance of cyber-warfare capabilities, with China supporting (publicly at least) a UN-supervised ban, while the US prefers the status quo in which it can continue to develop its capabilities (McCarthy 2019).

The Huawei paradox, combined with the politics of fear and blame during the Covid-19 pandemic of 2020, has amplified the different approaches of the US, with its lack of a governance framework for data security and opposition to multilateral solutions, and China, with its Cyber Security Law and support for global cyber governance. It appears the law of the cyber jungle will persist at the global level while, as will be discussed below, the European Union (EU), with its comprehensive Cybersecurity Act, General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS), models at a regional level the most advanced attempt at rules, norms and standards to guide cyber risk management.

4.3 Economic cooperation risk

The denial of supply of advanced semiconductor chips to Huawei by the US appears likely to reinforce China’s geopolitical fears of containment and indeed historic memories of dismemberment by outside powers. Consequently, it can be expected to drive China to double down on its strategy for not only self-reliance and alternative sources of supply but indeed dominance in next generation technologies. It may take some years, but China can be expected to develop a semiconductor industry to rival the US in time. While it is impossible to prove a counterfactual, it has been suggested by Kennedy (2020) that a more “principled interdependence” between US and Chinese supply chains rather than decoupling might have sustained US semiconductor leadership, slowed China’s technological advance and offered opportunities for joint work on risk management. Coercion has been chosen over cooperation in what may yet prove to be a turning point in the deteriorating geopolitical contest between the US and China, which was being extended to impact new firms and new industries at the time of writing.

The economic costs of excluding Huawei alone are considerable. A Huawei-commissioned Oxford Economics report (2019) predicted that restricting Huawei from competitive tenders will lead to increased 5G investment costs of between eight percent to 29 percent over a decade

and would have a cost to GDP in 2035 from \$2.8 billion in Australia to \$21.9 billion in the US. For US semiconductor firms, the export controls on sales to Chinese buyers constitute a major risk to their global business strategies. In a survey of exports in the first four months of 2018, Capri (2018) found Qualcomm relied on China for 60 percent of revenue, Micron over 50 percent and Broadcom about 45 percent. A Boston Consulting Group report forecast a full decoupling with China would reduce the US chip sector revenue by 37 percent and lower its market share to 30 percent, while China's market share would rise from three percent to 31 per cent (Varas/Varadarajan 2020). Further, as the geopolitical climate worsens, there is a risk that China will retaliate against US or allied firms. The Chinese government has reportedly drawn up plans to target so-called "unreliable entities", such as Fedex, which it is alleged allowed shipments of weapons to Hong Kong and mainland China and diverted US packages addressed to Huawei (Wu 2020). Any tit-for-tat economic coercion between China and the US will pose significant economic risks for third parties if it escalates, as expected, to include more expansive export controls, prosecutions of technology theft and restrictions on joint research and development with Chinese partners (Thomas-Noone 2020).

Farrell and Newman (2019) coined the phrases "weaponised interdependence" for this phenomenon of a state deploying economic coercion to leverage its asymmetrical power over a global network and "chokepoint effect" to deny network access to an adversary. Now that the US has set the precedent in its campaign against Huawei, how else the tactic might be deployed is not yet clear, with fears in China, for example, that the US could target international payments through its SWIFT system (Zhao 2020). To be sure, once the process is initiated against a firm or a sector, entire supply chains will be disrupted. The consequent evolution of a new global economy that moves away from market-led globalisation towards state-led spheres of geopolitical influence is uncertain at this point but 2020 may yet turn out to be a tipping point towards a much more geopolitically-infused international business environment. Geopolitical risk analysis is likely to receive much more attention in international business literature.

5 Risk assessment

The assessment of security, international relations and economic cooperation risks for 5G networks must be made in the context of not only contemporary international relations but over the life of such networks. This means planning for scenarios, including worst case scenarios. The theoretical capability for cyber-attack, for example, might not be a serious risk in some scenarios, but might become a threat in worst case scenarios in which the major powers are escalating confrontation or engaged in conflict. Following his Huawei ban, Australian prime minister, Malcolm Turnbull observed "it's important to remember that the threat is a combination of capability and intent. Capability can take years or decades to develop ... but intent can change in a heartbeat" (Bourke 2019). The Australian government clearly assessed the risk could become a threat, and therefore adopted a strategy of risk avoidance by banning Huawei all together. Based on distrust of the Chinese party state, the logic of this strategy would be to avoid all

critical supply dependencies on China, which has indeed become a common rallying call within the US and some of its allies since.

Any qualitative assessment of risks must take into account two key concepts, likelihood and consequence. The type of political risk will depend on whether the factors generating the risk arise at the firm level, the country level or as a result of the geopolitical environment. Huawei as a firm has been assessed to pose security risks because of the nature of the Chinese party state and the risks are therefore China risks, or geopolitical risks, rather than specific to the firm itself. Equally, the international relations risks that are generated by the case appear to be not simply because of Huawei itself but arise from the diverging interests of the US and China, characterised in particular by the lack of global governance rules, norms, standards and institutions, which have been established and maintained in other sectors, as noted above, from aviation to food security. Further, in relation to economic cooperation risks, Huawei again appears to be simply the trigger case for an emerging trend in the new geopolitical contest for the US and China to deploy economic coercion, to reconfigure supply chains and indeed to reshape globalisation according to geopolitical agendas and, consequently, abandoning the neoliberal and internationalist market-led phase of globalisation that characterised previous decades.

Accordingly, the Huawei case can be assessed as a prime example of geopolitical risk and can therefore only be understood in the context of the international relations, security and consequent economic policies of the major powers. Suppliers and partners of Huawei and indeed any strategically important firms from China or the US must therefore plan to manage geopolitical risks in the current environment. There has traditionally been very little cross-fertilisation between business literature on political risk and international relations literature (Fägersten 2015), yet this discussion demonstrates that risks for governments, firms and communities in the Huawei case are entirely bound up in questions of international relations and will require new approaches to risk management.

6 Risk management

Ideally, risk management in matters of security, in particular, should take a “zero trust” approach that is blind to suppliers and that applies layers of monitoring and testing for vulnerabilities, as threats could actually come from anywhere – not just one particular geopolitical competitor at any one time. Equally, risk management, whether in relation to security, international relations or economic cooperation risks, should ideally take place within established internationally agreed rules, norms and standards, as well as institutions for enforcement. In the new technologies, however, the US laissez-faire approach has dominated, although as discussed below the EU has introduced sophisticated regulations to protect against cyber risks that may provide a way forward.

Nevertheless, the risk of a major power acting to weaponise interdependence has now been demonstrated by the US campaign against Huawei and it is equally conceivable that China, too, could weaponise interdependence in the new technologies in which it leads. Neither major power is solely at risk here, and both have the capacity to generate risks. Other states will therefore make a proportionate risk assessment in relation to Huawei with an eye to the geopolitical environment, including in which context cyber and other risks are likely and in which context they would be of high consequence. Governments will also factor into their assessments whether subsequent actions are likely to impact on trust and cooperation with other countries, including both China and the US. In the absence of global rules and norms to build confidence in international cooperation and to minimise risks in 5G, governments must also build their technical capabilities to monitor and mitigate identified cyber risks. The technologies, including equipment, software and updates, are however so complex that it is simply not possible for technical monitoring to have any level of certainty that it will detect kill switches or malicious code, in particular if they have been implanted by the supplier (Lysne 2018).

The interplay between security and economic factors such as supply chains and trade and investment policies must also be weighed as part of any risk assessment and development of a risk management strategy. An EU coordinated risk assessment (European Commission 2020) noted that the technological change represented by 5G will increase the overall attack surface for potential cyber threats, across networks and in software development and update processes, as well as in relation to reliance on network operators and their role in the supply chain. Without naming Huawei, it drew particular attention to the importance of the individual risk profile of suppliers and the increased risk of dependency on a single supplier.

For governments that assess likely and consequential cyber risks but elect not to follow the Australian example of complete risk avoidance, capabilities must be developed or sustained to manage and mitigate identified risks. In the absence of global rules and norms, this remains an area of uncertainty and diversity in policy development, as well as in technical capacity-building. Each state will have sensitive assets and vulnerabilities and will need to ensure that it has regulatory, monitoring and technical capabilities to protect against risks to those sensitive assets and vulnerabilities. State security agencies need to develop and deploy extremely high system security strategies for cyber risk assessment and mitigation in an increasingly complex environment of global supply chains, involving thousands of actors and sources of software code. Further, to protect citizens from the risks posed by both Chinese and US firms, states will need data protection capabilities, with regular audits of data collection processes by international firms, ideally overseen by independent regulators.

It is unclear to what extent states are ready for the new cyber world.

The EU has become a leader in grappling with the new cyber-risk management challenges. Indeed, the EU has significant norm-setting power because of its highly developed system of international harmonisation across all sectors of the economy, and its capabilities to manage

risk in the digital economy may yet provide a model for others. It has introduced cybersecurity standards, including the GDPR to safeguard data integrity. The EU toolbox of risk mitigating measures includes strengthened regulatory powers and technical improvements to improve security of 5G networks and equipment, including restricting “high-risk” suppliers (originating in countries without democratic checks and balances) from providing core network assets and diversification of vendors to avoid dependency on one supplier. Further, it recommends strengthening local EU capacities to supply 5G and post-5G technologies (European Commission 2020). The provisions restricting core network services recognises that control of the core network is more valuable for espionage than non-core components, the latter only providing access in local areas (Taylor 2020).

There is however a danger in Europe, unlike the US, that telecommunications providers have neglected their capabilities to manage their own networks, often outsourcing to equipment vendors, including Huawei. Relying on Huawei to monitor cyber risks that some claim emanate from or through Huawei would appear to be unwise. Governments taking a risk management approach need to require service providers to maintain full service technical expertise and comprehensive security capabilities, and to ensure they maintain reliable monitoring capabilities, or to develop automated solutions (Hubert 2020).

Diversification of the supply chain offers an important risk mitigation measure. If at some time in the future, a particular supplier is identified as constituting a likely and consequential risk, it will be less costly to avoid risk if a diversity of suppliers is available and already present in the market. Nevertheless, as in most industry sectors, telecommunications supply chains are highly globalised and it is not only Chinese firms that source components from China, so it should be expected that governments will seek to diversify entire supply chains over time if they remain concerned about cyber risks emanating from China in particular. Equally, economic coercion risks emanating from the US export controls on its advanced semiconductors will force countries and firms not part of the US-led “Clean Network” to source new suppliers and to develop new supply chains, as is already underway (Capri 2020). A proposed Open Radio Access Network model may offer a future opportunity to allow multiple vendors to operate 5G services interchangeably, without one firm providing all of the infrastructure, but the model is as yet unproven.

To mitigate risks of espionage, encryption can be employed. Control over data integrity can also be strengthened (although not guaranteed) by requiring that data is stored within national borders rather than exported to other jurisdictions. China mitigates cyber risks (from, for example, the US), by requiring that all data storage is held within China’s national borders and is subject to its domestic cyber security legislation. To mitigate against cyber-attacks, duplication of critical functionality is one option, although costly, to allow for an alternative network to replace a compromised network (Lysne 2018). For those governments that can afford it, highly sensitive networks, such as emergency services and national security, can be maintained independently, although this also is an expensive option.

Finally, national governments have a widely recognised power to regulate trade and investment on national security grounds and this provides potential, although unexplored, opportunities in this case. Instead of a ban, for example, a government could approve a foreign supplier but only on the condition that it forms a new, domestically-based joint venture with a domestic firm that has adequate monitoring capabilities to mitigate cyber risks. Huawei has offered to license its technology to US firms (Friedman 2019) and presumably could be required to do so by other jurisdictions, with national firms building and operating the network, with rewritten source codes, inspections of equipment and software and other processes to meet national security requirements. Huawei has already moved to manufacture 5G network equipment in France for the European market (Huawei 2020).

7 Conclusion

The new technologies of the fourth industrial revolution are generating a whole new set of geopolitical risks. While Nye (2011) predicted cyber power would be more diffused than other forms of power, just as earlier observers expected of the information revolution, the shape of the world emerging in the 2020s remains the domain of the nation state. The dominant power, the US, is determined to maintain its position, including resisting global governance in cyber governance and in wielding the power of the state against the claimed risks of Huawei. Meanwhile, China is developing powerful cyber-capabilities to match its growing economic power and is seeking to set the agenda in global governance, yet it is deeply distrusted amongst liberal democracies in particular. In a rapidly deteriorating climate of geopolitical contest, confrontation and even conflict is no longer out of the question. Risks of cyber-espionage and sabotage, as well as weaponisation of information and artificial intelligence, therefore become assessed by states as realistic security threats. No rules or institutions exist to sanction rule-breaking or to rebuild confidence and trust. At the time of writing, it would appear the world is headed towards a spiral of decoupling strategically important supply chains and the potential construction of two rival systems, one led by the US and one by China.

Even in a decoupled world, security risks will remain and there is an urgent need for more technical research on risk management capabilities. At the national level, precautionary measures and enhanced risk management strategies are essential. These are likely to remain highly contested matters for some time to come.

To date, the digital economy has generated natural monopolies that control vast amounts of data, extract value and gather more and more power. These monopoly actors are now the largest firms in the world, and most originate from the US. The lack of governance of the digital economy raises a broader range of risks than China alone. Decision makers have failed to date to comprehensively grapple with the new rules that may be needed to reduce the risks of these natural monopolies seizing more power over governments, the economy and individuals.

The Huawei debate is not simply about the rise of one firm from China to threaten US supremacy. Huawei is a proxy for fear of China itself, its likely future capabilities and possible intentions. Whether China acts according to high risk or threat scenarios is, of course, heavily contingent on the state of the international system and whether it descends into conflict or whether international cooperation can be maintained.

The US and some of its allies appear to so deeply distrust China that they are unwilling to attempt to find new international rules, norms, standards and institutions to govern the new digital economy. We should be careful what we wish for. By branding China as an unacceptable risk and decoupling from its world-leading firms, rather than developing risk management strategies and systems of international cooperation, we may reinforce China's historical geopolitical fear of encirclement, and over time encourage its government and firms to behave in exactly the way we fear. Or, if the worst-case scenario analysts are correct, we could be headed in that direction anyway.

The Huawei paradox is therefore more than simply a problem of international business but represents a crisis of international relations, driven not only by trust in a supply chain, but the larger questions of whether it is possible to build processes of engagement, co-existence, norms, verification and enforcement to maintain international peace and security.

8 References

Alon, I. / Herbert, T. (2009): A stranger in a strange land: Micro political risk and the multinational firm. In: *Business Horizons*, 52(2), 127-137.

Alon, I. / Martin, M. (1998): A normative model of macro political risk assessment. In: *Multi-national Business Review*. https://www.academia.edu/668635/A_normative_model_of_macro_political_risk_assessment

Balding, C. (2019): Huawei Technologies' links to Chinese State Security Services. In: SSRN, 09.07.2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726

Biddle, S. (2020): The Filthy Hypocrisy of America's 'Clean' China-Free Internet. In: *The Intercept*, 06.08.2020. <https://theintercept.com/2020/08/06/the-filthy-hypocrisy-of-americas-clean-china-free-internet/>

Bourke, L. (2019): Turnbull warns Brits about letting Huawei build 5G network. In: *The Age*, 06.03.2019.

Bryan-Low, C. / Packham, C. / Lague, D. / Stecklow, S. / Stubbs, J. (2019): Special report – hobbling Huawei: Inside the U.S. war on China's tech giant. In: *Reuters*, 22.05.2019. <https://www.>

reuters.com/article/huawei-usa-5g/rpt-special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSL4N22Y02S

Cai, J. (2019): Will the China of tomorrow run on the technology behind bitcoin? In: South China Morning Post, 02.12.2019. <https://www.scmp.com/news/china/politics/article/3040132/will-china-tomorrow-run-technology-behind-bitcoin>

Capri, A. (2020): COVID-19 impact on business: will the pandemic trigger more state intervention in business strategies? In: Hinrich Foundation, 30.03.2020. <https://hinrichfoundation.com/trade-research/global-trade-research/thought-leadership/covid-19-impact-on-business-will-the-pandemic-trigger-more-state-intervention-in-business-strategies>

Chan, J. (2019): All may not be smooth along China's digital silk road. In: The Interpreter, 20.08.2019. <https://www.lowyinstitute.org/the-interpreter/all-may-not-be-smooth-along-china-s-digital-silk-road>

Chang, G. (2020): The Great U.S.-China Tech War. New York, NY: Encounter Books.

Dirks, E. / Cook, S. (2019): China's Surveillance State has Tens of Millions of New Targets. In: Freedom House China Media Bulletin, 139. <https://freedomhouse.org/report/china-media-bulletin/2019/china-media-bulletinkey-individual-police-databases-tiktok>

Dowden, O. (2020): Huawei to be removed from UK 5G networks by 2027. In: Department for Digital, Culture, Media & Sport/National Cyber Security Centre (Hg.): Press release, 14.07.2020. <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027>

Eisenstein, I. / Halpert, J. (2018): Data protection, privacy and security alert. In: DLA Piper Publications, 12.04.2018. <https://www.dlapiper.com/en/us/insights/publications/2018/04/us-cloud-act-authorizes-search-warrants-for-data-stored-abroad>

European Commission (2020): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU – implementing the EU toolbox. Brussels, 29.01.2020, COM(2020) 50 final. <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/01/POLITICO-5G-toolbox-Communication-of-the-EU-Commission-January-29-2020.pdf>

Fägersten, B. (2015): Political risk and the commercial sector - aligning theory and practice. In: Risk Management, 17(1), 23-39. <https://doi.org/10.1057/rm.2015.5>

Farrell, H. / Newman, A. (2019): Weaponized Interdependence: how Global Economic Networks Shape State Coercion. In: *International Security*, 44 (1), 42-79. https://doi.org/10.1162/isec_a_00351

Fernandes, C. (2019): What's at stake in Trump's war on Huawei: control of the global computer-chip industry. In: *The Conversation*, 01.10.2019. <https://theconversation.com/whats-at-stake-in-trumps-war-on-huawei-control-of-the-global-computer-chip-industry-124079>

Fitzpatrick, M. (1983): The definition and assessment of political risk in international business: a review of the literature. In: *The Academy of Management Review*, 8(2), 249-254. <https://www.jstor.org/stable/257752?seq=1>

Fletcher, B. (2019): Telenor ditches Huawei, taps Ericsson for 5G RAN in Norway. In: *Fierce Wireless*, 13.12.2019. <https://www.fiercewireless.com/5g/telenor-ditches-huawei-taps-ericsson-for-5g-ran-norway>

Friedman, T. (2019): Ren Zhengfei's Interview with New York Times Op-Ed Columnist Thomas L. Friedman. In: *Huawei Facts – Voices of Huawei*. <https://www.huawei.com/en/facts/voices-of-huawei/ren-zhengfeis-interview-with-new-york-times-op-ed-columnist-thomas-l-friedman>

Gilding, S. (2020): 5G choices: a pivotal moment in world affairs. In: *The Mandarin*, 09.01.2020. <https://www.themandarin.com.au/124337-5g-choices-a-pivotal-moment-in-world-affairs>

Girard, B. (2019): The real danger of China's national intelligence law. In: *The Diplomat*, 23.02.2019. <https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law>

Gu, L. (2019): China's Huawei, AU sign MoU to strengthen technical partnership on ICT. In: *English China News Service (ECNS), Sci-tech*, 04.06.2019. <http://www.ecns.cn/news/sci-tech/2019-06-04/detail-ifziupva1116191.shtml>

Hartcher, P. (2018): How China is driving Australia and Trump into each other's arms. In: *The Sydney Morning Herald*, 25.09.2018. <https://www.smh.com.au/politics/federal/how-china-is-driving-australia-and-trump-into-each-other-s-arms-20180924-p505mr.html>

Heater, B. (2020): Senate passes 'rip and replace' bill to remove old Huawei and ZTE equipment from networks. *TechCrunch*, 28.02.2020. <https://techcrunch.com/2020/02/27/senate-passes-rip-and-replace-bill-to-remove-old-huawei-and-zte-equipment-from-networks>

Hillman, J. / McCalpin, M. (2019): Watching Huawei's 'safe cities'. In: *Center for Strategic & International Studies (CSIS): CSIS Briefs*, 04.11.2019. <https://www.csis.org/analysis/watching-huaweis-safe-cities>

Hjortdal, M. (2011): China's Use of Cyber Warfare: espionage meets strategic deterrence. In: *Journal of Strategic Security*, 4(2), 1-24. <https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss>

Huawei (2020): Huawei announces it will open manufacturing plant for wireless products in France. In: *Press Release*, 27.02.2020. <https://huawei.eu/press-release/huawei-announces-it-will-open-manufacturing-plant-wireless-products-france>

Hubert, B. (2020): 5G: The outsourced elephant in the room. In: *berthub.eu*, 20.01.2020. <https://berthub.eu/articles/posts/5g-elephant-in-the-room>

Hunter, F. (2019): New communications minister denies Huawei ban will hurt Australia's 5G rollout. In: *The Sydney Morning Herald*, 13.06.2020. <https://www.smh.com.au/politics/federal/new-communications-minister-denies-huawei-ban-will-hurt-australia-s-5g-rollout-20190612-p51wup.html>

Ikenson, D. (2019): Blacklisting Huawei could cost trillions, so let's look before we leap. In: *China-US Focus*, 05.07.2019. <https://www.cato.org/publications/commentary/blacklisting-huawei-could-cost-trillions-so-lets-look-we-leap>

Jarvis, D. (2008): Conceptualizing, analyzing and measuring political risk: the evolution of theory and method. In: *Lee Kuan Yew School of Public Policy Research Paper Series LKYSPP08-004*. <http://dx.doi.org/10.2139/ssrn.1162541>

Kennedy, S. (2020): Washington's China Policy Has Lost Its Wei. In: *Center for Strategic & International Studies (CSIS): CSIS Briefs*, 27.07.2020. <https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei>

Kobrin, S. (1979): Political risk: a review and reconsideration. In: *Journal of International Business Studies*, 10, 67-80. <https://doi.org/10.1057/palgrave.jibs.8490631>

Li, L. / Cheng, T. / Yu, Y. (2020): How a handful of US companies can cripple Huawei's supply chain. In: *Nikkei Asian Review*, 19.08.2020. https://asia.nikkei.com/Spotlight/Huawei-crackdown/How-a-handful-of-US-companies-can-cripple-Huawei-s-supply-chain?del_type=1&pub_date=20200819190000&seq_num=7&si=83867

Lim, D. / Ferguson, V. (2019): Huawei and the decoupling dilemma. In: *The Interpreter*, 28.05.2019. <https://www.lowyinstitute.org/the-interpreter/huawei-and-decoupling-dilemma>

Lysne, O. (2018): *The Huawei and Snowden Questions. Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment?* Fornebu, Norway: Simula Research Laboratory/Springer Open. <https://doi.org/10.1007/978-3-319-74950-1>

McCarthy, S. (2019): Could China's strict cyber controls gain international acceptance?. In: South China Morning Post, 30.09.2019. <https://www.scmp.com/news/china/diplomacy/article/3030758/could-chinas-strict-cyber-controls-gain-international>

McKenzie, N. / Galloway, A. (2020): The man who stopped Huawei: a former spook speaks out. In: The Sydney Morning Herald, 31.01.2020. <https://www.smh.com.au/national/the-man-who-stopped-huawei-a-former-spook-speaks-out-20200131-p53wi6.html>

McMaster, H. (2020): How China Sees the World. In: The Atlantic, 19.05.2020. <https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088>

Mikhailova, A. (2020): United States presents Britain with fresh intelligence on Huawei risks in last-ditch attempt to block deal. In: The Telegraph, 13.01.2020. <https://www.telegraph.co.uk/politics/2020/01/13/united-states-presents-britain-fresh-intelligence-huawei-risks>

Nye, J. (2011): The Future of Power. New York, NY: Public Affairs.

Oxford Economics / Huawei (2019): Restricting Competition in 5G Network Equipment: An Economic Impact Study. https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V7.pdf

Perez, B. (2019): UK approves Huawei's restricted use in 5G networks. In: South China Morning Post, 28.01.2019. <https://www.scmp.com/tech/big-tech/article/3047945/uk-approves-huaweis-restricted-use-5g-networks-handing-lifeline>

Pham, S. (2019): Huawei sues US government over new FCC restrictions. In: CNN Business, 05.12.2019. <https://edition.cnn.com/2019/12/05/tech/huawei-us-ban-lawsuit/index.html>

Polyakova, A. (2019): Rules Based Audio [Audio podcast]. In: The Interpreter, 17.12.2019. <https://www.lowyinstitute.org/the-interpreter/exporting-digital-authoritarianism-podcast-out-now>

Robock, S. (1971): Political risk: identification and assessment. In: Columbia Journal of World Business, 6(4), 6-20.

RWR Advisory Group (2019): Assessing Huawei Risk: how the track record of the CCP should play into the due diligence of Huawei's partners and customers. RWR Reports. <https://www.rwradvisory.com/assessing-huawei-risk>

Sachs, J. (2018): The War on Huawei. In: Project Syndicate, 11.12.2018. <https://johnmenadue.com/jeffrey-d-sachs-the-war-on-huawei-project-syndicate-11-12-18>

Schia, N. / Gjesvik, L. (2017): China's cyber sovereignty. In: Norwegian Institute of International Affairs (NUPI)(Hg.): Policy Brief 2/2017. <http://hdl.handle.net/11250/2434904>

Snowden, E. (2019): Permanent Record. New York, NY: Henry Holt and Co.

Soo, Z. / Zhang, J. (2020): Cybersecurity at Top of Huawei's Agenda as Europe Decides on 5G Infrastructure. In: South China Morning Post, 13.04.2020. www.scmp.com/tech/big-tech/article/3079455/cybersecurity-top-huaweis-agenda-europe-decides-5g-infrastructure

Sottilotta, C. (2017): Rethinking political risk. New York, NY: Routledge.

Stockton, N. (2020): China Launches National Blockchain Network in 100 Cities. In: IEEE Spectrum, 20.03.2020. <https://spectrum.ieee.org/computing/software/china-launches-national-blockchain-network-100-cities>

Sykulski, L. (2014): Geopolitical risk in the analysis of international relations. In: European Journal of Geopolitics, 2, 132-144. https://www.academia.edu/39847124/EUROPEAN_JOURNAL_OF_GEOPOLITICS_2_2014_Leszek_Sykulski_GEOPOLITICAL_RISK_IN_THE_ANALYSIS_OF_INTERNATIONAL_RELATIONS

Taylor, M. (2020): Why the UK is right to use Huawei 5G technology. In: Verdict, 28.01.2020. <https://www.verdict.co.uk/huawei-5g-uk-technology>

Thomas-Noone, B. (2020): Tech Wars: US-China Technology Competition and What it Means for Australia. In: United States Studies Centre, 16.06.2020. www.ussc.edu.au/analysis/us-china-technology-competition-and-what-it-means-for-australia?utm_medium=email&utm_campaign=PUBLICATION%20ALERT%20%20Australia%20left%20vulnerable%20in%20US-China%20tech%20war&utm_content=PUBLICATION%20ALERT%20%20Australia%20left%20vulnerable%20in%20US-China%20tech%20war+CID_30ef124862712d92ca0d39a536a11a61&utm_source=USSC%20Campaign%20Monitor&utm_term=Tech%20wars%20US-China%20technology%20competition%20and%20what%20it%20means%20for%20Australia#australia-and-the-evolving-us-china-struggle-for-technological-advantage

U.S. Department of Commerce (2020): Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List. In: Press release, 17.08.2020. <https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and>

U.S. Department of Justice (2019): Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Fraud, and Obstruction of Justice. In: Justice News, 28.01.2019. <https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade>

U.S. Department of State (2020): The Clean Network Safeguards America's Assets. In: Fact Sheet, 11.08.2020. <https://www.state.gov/the-clean-network-safeguards-americas-assets>

Varas, A. / Varadarajan, R. (2020): How restricting trade with China could end US semiconductor leadership. In: Boston Consulting Group, 09.03.2020. <https://www.bcg.com/en-hu/publications/2020/restricting-trade-with-china-could-end-united-states-semiconductor-leadership.aspx>

Wang, Y. (2020): Upholding Multilateralism, Fairness and Justice and Promoting Mutually Beneficial Cooperation. Keynote speech at the International Seminar on Global Digital Governance. Beijing, 8.9.2020. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/2461_663310/t1812950.shtml

Weiss, J. (2019): A world safe for autocracy? In: Foreign Affairs, 98(4), <https://www.foreignaffairs.com/articles/china/2019-06-11/world-safe-autocracy>

Wernick, D. (2006): Terror incognito: international business in an era of heightened geopolitical risk. In: Suder, G. (Ed.): Corporate strategies under international terrorism and adversity. Cheltenham, UK: Edward Elgar. 59-82.

Whalen, J. / Fifield, A. (2019): China's Huawei may need two to three years to recover from U.S. trade ban, CEO says. Washington Post, 12.12.2019. <https://www.washingtonpost.com/business/2019/12/12/chinas-huawei-may-need-two-three-years-recover-us-trade-ban-ceo-says>

Wu, W. (2020): Why China did not retaliate after latest US move to target Huawei. In: South China Morning Post, 13.06.2020. <https://www.scmp.com/news/china/diplomacy/article/3088826/why-china-did-not-retaliate-after-latest-us-move-target-huawei>

Zenglein, M. / Holzmann, A. (2019): Evolving made in China 2025: China's industrial policy in the quest for global tech leadership. In: Mercator Institute for China Studies (MERICS), 02.07.2019. <https://www.merics.org/en/papers-on-china/evolving-made-in-china-2025>

Zhao, C. (2020): Using SWIFT settlements to threaten China will backfire. In: Global Times, 30.06.2020. <https://www.globaltimes.cn/content/1193106.shtml>

Zheng, W. (2019): China's Shenzhen is using big data to become a smart 'socialist model city'. In: South China Morning Post, 01.11.2019. <https://www.scmp.com/news/china/politics/article/3035765/chinese-city-shenzhen-using-big-data-become-smart-socialist>

Beat Habegger

Political Risk Management as an Imperative for the Insurance Industry – and Beyond



Beat Habegger
Swiss Re

Abstract

Nicht nur, aber auch in der Versicherungswirtschaft nehmen politische Risiken eine wichtige Position unter Top-Managerinnen und Managern ein. Da sich die Versicherungsindustrie sehr unmittelbar mit politischen Risiken auseinandersetzen muss, ist sie auch gefordert, diese zu verstehen. Dieser Beitrag diskutiert, wie Versicherungen mit politischen Risiken konfrontiert sind, wie sie diese versuchen zu analysieren und zu managen. Aber es werden auch bedeutende Unterschiede zwischen Versicherungen und anderen Unternehmen thematisiert, um hervorzuheben, was andere Unternehmen von Versicherungen lernen können.

Not only, but also in the insurance industry have political risks assumed a prominent position in the rankings about the most relevant concerns for executives. Since the insurance industry is very immediately dealing with political risks and needs to understand their very nature, this paper discusses in which ways insurers are confronted with political risks, and how they try to understand and manage these risks. However, also important differences between insurers and other companies are highlighted to understand, what the latter can learn from insurance companies.

1 Introduction

Business executives have ranked political risks among their top concerns for many years. Geopolitical instability, for example, has been consistently mentioned as a top potential risk to global economic growth by business leaders across the globe in the McKinsey economic conditions snapshots since at least 2014. In 2019, it still holds on to second spot, topped only by trade conflicts. Year after year, The Global Risk Reports from the World Economic Forum also points to the “unsettled geopolitical landscape” (WEF 2020: 10) due to various risks with the potential to have a major impact on the economy and society at large. The business community’s awareness of political risk has increased and many companies have realized that the assumption of a stable “strategic status quo” (Chipman 2016) is an illusion. The management of political risk, however, is still neglected in many corporate headquarters and boardrooms.

The insurance industry is uniquely exposed to political risks in several ways. In the core insurance business, companies can provide coverage for incurred damage due to political risks – sometimes explicitly, sometimes silently. In order to financially cover future losses, they collect premiums from clients. These premiums are invested in financial markets, which are impacted by factors such as political actions. Finally, insurance is a heavily regulated industry: capital and solvency requirements as well as market behavior are tightly supervised by government

authorities and the business model based on global diversification across politically volatile markets is vulnerable to protectionist policies.

Taken together, these factors highlight the relevance of political risks for the insurance industry. Due to this unique exposure, and because knowledge of how to manage risk is the industry's "raw material", the insurance sector has developed specific experience and expertise in dealing with political decisions and actions that have an impact on the financial and strategic condition of companies. In this article, we briefly outline why companies should care about politics. We then show specifically how insurers are exposed to political risk. We continue by describing how they manage their political risk exposure and protect themselves against financial losses triggered by political risk. Finally, we close by highlighting some challenges for the future.

2 Why should companies care about politics?

Politics sets the legal and regulatory boundaries within which companies operate. It thus defines the rules that the various actors have to comply with. Political intervention occurs in any business environment: in democracies and dictatorships, in free-market systems and under central planning, and in developed and developing economies. Everywhere, individuals and social groups – including companies – compete for access to and use of resources, and fight for their interests and values. Political actions and decisions thus have an influence on determining the interests and values that prevail, and how resources are allocated and distributed in society. The drivers of political actions and decisions are not only governments; there are many other "risk generators" (Rice/Zegart 2018) in public policy, the economy, and society at large that widen the array of politically-minded actors who have an impact on business.

Companies cannot escape politics. They are affected by decisions of governments and other actors who influence their ability to make profits – both positively and negatively. They must engage with their external environments as a result of uncertainty about what policy will look like, how it will change, and how the future will eventually play out. Due to this uncertainty, and the human agency that is always involved in politics, we call it a political risk. This risk can be conceptualized like any other form of risk: (1) the probability that a politically induced event or decision occurs within a specific time frame; and (2) the expected gain or loss that the company faces as a result.

The focus on political risk means looking at politics from the perspective of a company as a commercially driven enterprise. The lens through which a corporate political risk analyst looks at political developments is therefore different compared to an analyst working in academia or for a government or a non-governmental organization (NGO).

In *academia*, the interest in politics is an empirical one. The essential goal is to find answers to 'why' questions. For instance, 'why is a political actor taking that particular decision?', or 'why

have political events unfolded in the way they have?' In *government* or *NGOs*, on the other hand, the overriding question is 'what do we need to do?' They might want to decide how to defend the interests of citizens or stakeholders, or how to solve a particular public policy problem. The focus thus shifts from an empirical interest to a normative one; the goal is to provide actionable guidance for public policy decision-makers and to steer them in the desired direction.

For *companies* the relevant questions are 'what is likely to happen?' and 'what can we do about it?' The analytical interest is neither empirical (although it may also be important to understand why something happens) nor normative (although companies may also try to influence policy decisions when they can); the focus, rather, is on providing concrete support for corporate decision-making in order to preserve revenues, earnings, and the balance sheet. The key questions are 'what is going to happen in the world of politics?' and 'what will this mean for our company?' The corporate political risk analyst focuses on developing useful forecasts that help people to understand the likely trajectories of political action. By doing so, they support corporate decision-makers in preparing for and mitigating against adverse impacts on their business.

3 The exposure of insurance companies to political risk

The insurance industry is particularly exposed to political risks. It explicitly or silently underwrites insurance liabilities covering political risks. It invests earned premiums on financial markets impacted by political risks and operates a heavily regulated and supervised business model based on global diversification, and which is vulnerable to protectionist policy.

3.1 Underwriting political risks

As risk is the industry's "raw material", it has found various ways to offer insurance solutions for political perils. As with other risks, insurability depends on a set of criteria that need to be fulfilled, including the randomness of events, the ability to reasonably estimate the frequency and severity of uncertain future events, a large number of similarly exposed risks, and the ability to achieve a price that covers claims, administrative expenses, and capital costs (Braun/Fischer 2018: 47). If the insurance industry is able to hedge accumulation risks and loss potential, it is able to offer coverage for any kind of risk, including political risk.

The industry generally offers solutions for political perils with limited loss impact and limited frequency. A good example is insurance coverage for social unrest such as strikes, riots, and other forms of civil disturbance that may result in property damage. The industry has also found ways to offer coverage for certain perils under the condition that governments stand in as lender of last resort in case of high-severity events. The prime example here is terrorism insurance. While terrorism was for a long time considered to be insurable in a similar way to social unrest, the terrorist attacks on the United States in 2001 and the resulting catastrophic insurance loss changed the industry's assessment. The increased terrorism threat made it only viable for the

private insurance market to continue offering coverage if governments provided support in the form of risk pools¹ with state-guaranteed back up capacity for extreme events and compulsory insurance schemes. Further, some political perils largely remain excluded from insurance protection. An example is war, which is excluded from coverage in many traditional insurance policies, especially in property insurance, due to the extreme risk accumulation potential. Even in case of war, however, some coverage is sometimes provided, for example in life and health insurance or in transport (marine) insurance for movable goods for a limited amount of time that allows ships to sail away from conflict zones before coverage expires.

While protection against political risks is usually part of a broader insurance scheme (e.g. a property insurance policy), Political Risk Insurance (PRI) products offer the opportunity to insure against certain types of political risks on a standalone basis. The PRI market has developed out of the traditional credit insurance market (for an overview see Heaney/Nijhout 2018). It offers bespoke solutions for perils such as government expropriation or sovereign non-payment risks and targets companies investing abroad or banks seeking protection when financing cross-border projects or shipments. Usually, the insurable perils are grouped into four categories: (a) confiscation, expropriation, or nationalization by the host government without due compensation; (b) currency inconvertibility that deprives a foreign investor of the possibility to repatriate profits or dividends out of the country; (c) political violence, i.e. the destruction of assets due to politically motivated acts of violence; and (d) contract frustration when foreign governments (or sub-sovereign entities) fail to honor a contract with a foreign investor (Tanner/Lier 2007: 21).

When underwriting political risk, it is also important to look beyond directly insured political perils such as those mentioned above. The “political characteristics” of an insured asset or an insured counterparty, i.e. the commercial entity or person that buys insurance protection, needs to be considered as well. Examples are, firstly, credit risk taken on governments or sovereign obligors such as ministries of finance or defense, sub-sovereign entities such as regional governments, but also state-owned banks or corporations, which have a different risk profile to privately held companies. Secondly, credit risks taken on private companies that a country regards as strategically important (either as a firm or an industry) are often more exposed to political intervention. Thirdly, insurance protection for assets that a country deems to be of strategic importance, for example specific infrastructure, pipelines, or natural commodities, could be exposed to higher political risk. Finally, in the realm of life and health insurance, politically exposed persons such as high-ranking politicians, or their family members, have a risk profile that is distinct from other persons and, consequently, must be properly assessed before granting insurance protection.

3.2 Investing premiums on financial markets

The insurance industry is not only vulnerable to political risk in the form of insurance losses, it is also exposed to political events and developments that lead to a decline in capital markets.

¹ Primary insurers issue separate terrorism policies that are ceded to the terror pool. Losses facing the terror pool are borne by the insurers participating in the pool in relation to their market share.

Insurers are asset managers. They collect premiums from clients and invest them in financial markets until they are used for covering losses. Insurers are thus vulnerable to political risks to the extent that they depreciate the value of an insurer's investment portfolio (either in economic or in accounting terms). In addition, insurers are also exposed to market declines with their own equity.

Political risk events drive market returns – at least in the short term – and capital markets tend to react negatively to international crises or major conflicts. However, while major events, including for example terrorist attacks, can lead to a sudden dip in markets, assets often quickly recover once the shock is over. Some observers have even pointed to the “war rally” phenomenon that benefits certain sectors such as the defense industry (while others, including the airline or tourism industries are obviously hurt). Other findings include that political events have a stronger impact on emerging economies than on developed economies, and that crises affecting strategic goods or raw materials (e.g. oil) leave clear traces on global markets (Tanner/Lier 2007: 26, 32). While the relationship between political events and capital markets is complex, it is obvious that insurers are exposed to capital market movements driven by political risks in relation to both their investment portfolios and their own equity.

3.3 Operating a business exposed to political threats and interventions

Beyond political risk exposures in underwriting and investment portfolios, all companies are exposed to political risks in relation to their business operations. First of all, an insurer's operational exposure is not fundamentally different from that of any other company, including in other industries. Companies generally face legal, regulatory or IT security risks that can originate in the public policy domain. Insurance companies could, for example, face politically-motivated violence and cyber-attacks, or state-sponsored industrial espionage, directed at its property, personnel, and systems – either as explicit targets or victims of collateral damage. International sanctions levied against individuals or companies by international organizations (e.g. the UN and the EU) or powerful countries (e.g. the US or UK) can distort business relationships in any sector and any company. The financial sector is particularly at risk given its involvement in financing arrangements across all industries and the often cross-border nature of its business.

Insurance is part of the highly regulated financial services industry. As such, it is exposed to political risk in the form of new laws and regulations that influence the legal order within which business is conducted. At the core of this are the so-called prudential measures that define how much capital companies need to hold to ensure that they can honor their financial obligations even in the case of large losses. Regulatory and supervisory frameworks are implemented to compel companies to adhere to capital and solvency rules, as well as to expected market behavior (conduct) to protect consumer trust in financial services.

While rules and regulations are usually codified at the national level, their emergence is often heavily influenced by transnational developments and shaped by international – or even

supranational – organizations. Finance is an international business and value creation can be particularly high in insurance when risks can be spread and diversified across broad geographies. Large insurers and reinsurance companies in particular operate a business model that is built on the ability to spread risk globally, including across politically volatile markets, to assume very large and complex risks (Swiss Re 2016: 17). Political decisions can hinder companies in performing this important function. Regulatory fragmentation (i.e. a lack of international standards) and the existence of protectionist measures intended to benefit national players to the detriment of international competitors, as well as barriers to market access (e.g. inability to operate on a cross-border basis, limited contract certainty, and limitations on the free flow of capital) are common in many countries, including in developed economies (Swiss Re 2016: 18). Such restrictions hinder the global insurance/reinsurance industry in its ability to offer its services, and societies thus forego the economic benefits of global diversification.

4 The political risk framework in insurance

As set out above, insurance companies are vulnerable to political risks on both sides of their balance sheets – on the liability and the asset side – as well as in their income statement and in relation to operating their business. Political risks are part of the highly diverse risk landscape facing insurers. In the case of Swiss Re, for example, emerging threats and opportunities are identified and assessed across a broad spectrum of risk categories. This encompasses core insurance risks (property and casualty, life and health) and financial risks (market risks and credit risks), as well as many other significant risks, including operational, liquidity, model and valuation, regulatory, strategic, sustainability, and political risks (Swiss Re 2020: 68). It is imperative for insurers to systematically manage all of these risk categories; political risk is no exception.

Nevertheless, individual risk categories have their own specific characteristics and require suitable risk management approaches. In the case of political risk, at least three aspects need to be specifically considered. Firstly, they belong to the group of risk categories that cannot be measured, quantified, and modeled in the same manner as risks such as natural catastrophes or longevity risks. Secondly, while political risks are sometimes directly insured, they are more often drivers of other risk categories which have an impact on property risks (e.g. social unrest leading to property damage), credit risks (e.g. regime change triggering non-payment of sovereign obligations), or reputational risks (e.g. human rights violations which put the continuation of business in a particular market into question). At first glance, the political origin of a specific risk event which leads to property damage or a credit default can easily be overlooked; it may also not be classified as a political risk event in companies' systems and processes. This can create the impression that political risks are of secondary importance; in reality, however, the impact is often simply less visible due to interdependency with other risks. Thirdly, the pervasiveness of political risk across insurance companies' business models and the entanglement with other risk categories means that substantial interdisciplinary expertise is required to be able to manage it effectively. Insurance knowledge, an understanding of economics and regulation, expertise in

public policy and security as well as strong cross-departmental cooperation within the company are cornerstones of effective political risk management.

Companies and other organizations usually resort to establishing frameworks in order to organize the way in which they approach risks. Below we propose focusing on four competencies that companies need to be able to manage political risks effectively: identifying risk; assessing risk; mitigating risk; and ensuring the right management capabilities are in place.

4.1 Scanning the horizon – identifying political risk

The first step is to identify any political risk to which the company could be exposed and that potentially impacts its performance. The goal is to make known risks fully transparent, to reduce any blind spots, and to detect emerging risks at an early stage in order to sketch out a comprehensive political risk landscape. This transparency allows corporate decision-makers to define their political risk appetite – how much risk are they willing to accept? – and to decide on the appropriate mitigation strategies.

Risk identification starts with continuously monitoring political developments in all relevant countries and markets. Monitoring should not be too narrowly defined geographically in order that cross-border spill-over effects are not missed in an interdependent world. It is not sufficient to focus on markets where the company has a local footprint, for example in the form of production facilities. It is essential to look at the country's profile in a regional context as well as to check supply chains or sales channels on a global basis. The same applies to the scope of relevant political perils given the knock-on effect of political developments on insurance or financial market risks. Moreover, the transmission mechanism between political trends or events and a company's commercial activities can sometimes be direct and clear-cut, but can also sometimes be indirect and hidden. Finally, it is essential that the identification of political risks is well integrated into a company's overall early risk detection or emerging risk management process, as it is the case, for example, with regard to Swiss Re's Sonar process and publications.²

4.2 Understanding your exposures – assessing political risk

Once political risks are identified, they must be understood. In line with the concept of risk as outlined above, the analyst thus assesses (a) the *likelihood* that a risk materializes in a specific form and within a specific time frame, and (b) the possible *impact* that the identified risk could have on the company. By doing so, the company understands what is at stake and can estimate its level of preparedness given the forecasted scenarios.

As political developments are always human-induced, the assessment of political risk starts with identifying the individuals or groups involved and their preferences. Analysts need to under-

2 <https://www.swissre.com/institute/research/sonar.html>

stand what they want to achieve (e.g. policy change, regime change, religious motivations, and accumulation of wealth) and what means they may use to get what they want (e.g. winning an election, overthrowing a government, and terrorizing the population). It is also relevant to assess what resources they possess (e.g. reputation, money, and relationships) and what constraints they may face (e.g. domestic opposition, international constraints, and lack of resources) in order to assess the likelihood of their success. The political risk analyst uses this assessment to develop a forecast – or several forecasts for different scenarios – that sketches out a trajectory into the future. This should not be confused with predicting the future; no one can know what the future holds and it is misleading to pretend to. However, analysts owe decision-makers an appraisal of the best estimate across a range of possible outcomes and must support them in thinking about alternative futures (Nye 1994: 88).

In order to facilitate the assessment of countries' risk profiles, companies often use indicators that provide insights into the quality of political institutions and democracy, freedom and human rights, terrorism and war risk, corruption perceptions, human and social capital, the ease of doing business, and the exposure to geopolitical risk. Many international governmental and non-governmental organizations make such information publicly available. Companies need to be clear about the indicators they want to use and the purposes for which they want to use them; some may also combine various sources into a bespoke rating that efficiently matches a specific commercial need. Swiss Re, for example, produces its own country political risk ratings, which are updated quarterly, to steer underwriting parameters for political perils, as well as to provide an information platform for use when exploring business and investment opportunities. Social media monitoring to follow key trends and to detect emerging risks is also becoming commonplace in many organizations. And, more recently, frameworks have been developed around Environmental, Social, and Governance (ESG) indicators that are also useful in monitoring political risks at the interface to sustainability management.

After making the forecast(s) and estimating the associated likelihood, the next step is assessment, which requires exploring what the impact might be on the company's balance sheet. To do this companies need to know "which assets are most valuable and which are most vulnerable" (Rice/Zegart 2018). While quantifying vulnerability is often not straightforward, it is possible to make approximate estimates. With regard to underwriting exposures, relevant questions include asking what markets might be at risk; what insurance lines might be particularly exposed; what types of insurance policies are usually written; whether insurance coverage would be triggered and what exclusions or other mitigating factors are in place; and what the company's current exposure actually is expressed in financial figures. Similarly, with regards to financial market impact, questions include what asset classes are most likely to suffer; what the likely range of market movements might be; and what the company's current portfolio looks like. In addition to this, operational constraints and associated costs for the company can also be weaved into the assessment. Taken together, it then becomes possible to build up an overall picture of the company's vulnerability to the forecasted scenarios.

4.3 Deciding on your response: mitigating political risk

In a third step, the company needs to decide how much risk it is willing to take and how it wants to respond to political risks. Companies will obviously have limited or no opportunity to influence the likelihood of a forecasted policy outcome; this is to a large extent the prerogative of governments and other actors who have direct leverage over public policy decisions. A company, however, can hedge against the inevitable negative impacts of certain political actions and decisions.

Hedging against risk is not a primary responsibility of political risk management. The task of considering and deciding on mitigation actions is carried out in other departments – in the case of insurance companies it is primarily the responsibility of insurance underwriters or investment managers – or staff in other specialized departments (e.g. legal or IT). However, political risk management – like any other risk management function – can provide an outline of the spectrum of available options on the basis of its assessments and propose the most meaningful measures. It is then up to the risk takers or decision-makers to decide.

It is obviously not possible to specify all of the measures that companies can take. Let us instead mention a few examples specific to the insurance industry. If a company wants to *avoid* exposure to a specific political risk in a particular market, it can fully withdraw from that market or hold back from making planned investments; it can exclude coverage of a political peril in its insurance contracts; or it can sell all of the assets that are at risk. If a company wants to *reduce* exposure to political risk (which is likely to be the prevalent case), it can take specific underwriting measures (e.g. reducing its share, and adjusting contractual clauses) or hedge the investment portfolio with adequate financial instruments. Portfolio diversification both on the underwriting and investment side are bread-and-butter strategies in insurance and also mitigate against political risk; diversification also counts in the form of operational redundancies (e.g. spreading location risk), while this obviously also comes at a cost. Another option is to cultivate good relationships with governments and continuously engage with policy-makers, if possible, to steer their decisions in a more desirable direction. The company may also use trade associations to initiate an industry-wide push to strengthen its clout. In some situations, companies may also be able to *transfer* some of the political risk to third parties. This can be done by resorting to external vendors or contractors. Another option for corporations and banks engaged in cross-border business is to buy political risk insurance. Insurance companies themselves may seek to protect their portfolios and peak risks by resorting to reinsurance solutions or, in the case of a reinsurer, by using retrocessions, i.e. passing some of the incurred risk on to another reinsurer.

4.4 Putting the right capabilities in place

Political risk management carried out using the three steps outlined above requires having the necessary management capabilities. This starts with staffing the team with professionals that have strong expertise extending into the fields of politics, economics, and business. They also

need to be able to deploy a broad range of analytical and methodological skills, including in strategic foresight, scenario development, and other forward-looking techniques. What is more, they need strong communication and reporting skills to be able to clearly articulate their analysis to decision-makers. Given improved availability of data and data processing tools, quantitative assessments are increasingly complementing established elements of political risk analysis, which have tended to be qualitatively-oriented. Analysts should also have a good understanding of the respective industry, market trends, and the regulatory and legal frameworks within which companies operate.

Securing access to reliable sources of information and data is crucial. Besides open-source intelligence from academia, thinktanks, international organizations, and specialized non-governmental organizations, analysts may also draw on their personal networks as well as on specialized commercial firms that provide political risk information and analysis (The Economist 2016: 57). There has been a boom in companies offering political risk advice in recent years and it is essential to carefully evaluate the type of products and services available (e.g. off-the-shelf versus bespoke analysis, geographic reach and coverage, on-the-ground presence or not, and seniority of analysts) and their quality in order to ensure that they match the company's needs. The right team with the right portfolio of competencies and access to relevant information then needs to carefully evaluate who the team's products and services are aimed at. This ensure the delivery of bespoke assessments and mitigation strategies that are aligned with the company's strategy, products, investments, and operational set-up.

5 The way forward: strengthening the focus on politics in corporate management

Insurers have certain advantages over companies in other sectors when it comes to dealing with political risk. Insurers are uniquely exposed to political risk as it not only has an impact on the operational functioning of the company, but also a direct impact on its assets (invested premiums) and liabilities (risk underwriting exposures). Risk is also an insurer's raw material. They build their commercial offerings around uncertain future events that could lead to material losses. Insurers are therefore well practiced in managing risks and using them for their own commercial propositions. Nevertheless, even in the insurance industry, awareness of political risk is not as widespread as might be expected.

A key reason for this are the interdependencies with other risk factors that tend to overshadow the political drivers behind property damage, mortality events, market movements, and credit losses. As commercially driven organizations, companies also have a strong tendency to look at the world through a "market lens" and to overemphasize economic considerations and rationalities in their analyses. Focusing on income, growth, and inflation can obscure threats from other sources such as emerging laws, the rise of new political actors, or the instability of political institutions (Bremmer 2005: 2). It is crucial to consider these factors and to actively

include them in multi-factor analyses that embrace politics as a key feature of companies' operational and strategic management.

There needs to be greater emphasis on political risk management when it comes to companies' strategy development. Targeted input on key markets, transnational developments, and global trends can be harnessed to develop a more effective corporate strategic roadmap. It helps to identify threats to the business and operating model and it may even uncover hidden opportunities for differentiating from competitors. To this end, political risk management must be able to continuously frame political developments in the context of corporate strategy and the market environment in which the company operates. It requires access to decision-makers; and, in turn, decision-makers need to develop an interest in the political landscape to understand what is happening outside the market space that could potentially derail their business.

Integrating politics does not mean crowding out other perspectives. Corporations already tend to work in compartmentalized ways, creating silos that do not talk and work together with each other enough. The goal is to increase the ability to pull various perspectives together by developing and cultivating a multi-disciplinary approach that synthesizes political risk with macroeconomic risk, financial market risk, legal risk, and so on. This helps to avoid an over-emphasis on certain risk factors, especially due to the "market lens" problem described above, and results in a more comprehensive, well-rounded risk picture.

6 References

Braun, Alexander / Fischer, Marius (2018): Political Risk Perils and Insurance Covers. In Braun, Alexander / Fischer, Marius (eds.): Handbook of Political Risk Insurance. St. Gallen: University of St. Gallen, 33-48.

Bremmer, Ian (2005): Managing Risks in an Unstable World. In: Harvard Business Review, June 2005, 2-9.

Chipman, John (2016): Why Your Company Needs a Foreign Policy. In: Harvard Business Review, Sept 2016, 36-43.

Heaney, Paul / Nijhout, Rob (2018): The Market for Political Risk Insurance. In: Braun, Alexander / Fischer, Marius (eds.): Handbook of Political Risk Insurance. St. Gallen: University of St. Gallen, 65-92.

Nye, Joseph S. (1994): Peering into the Future. In: Foreign Affairs, 73(4), 82-93.

Rice, Condoleeza / Zegart, Amy (2018): Managing 21st-Century Political Risk. In: Harvard Business Review, May/June 2018, 130-138.

SONAR: <https://www.swissre.com/institute/research/sonar.html>

Swiss Re (2020): Financial Report 2019. Zurich. <https://reports.swissre.com/2019> (30 September 2020).

Swiss Re (2016): The Benefit of Global Diversification: How Reinsurers Create Value and Manage Risk. Zurich.

Tanner, Rolf / Lier, Marco (2007): Political Risk and Insurance: Challenges and Opportunities in a Globalised World. Zurich: Swiss Reinsurance Company.

The Economist (2016): Risk Premiums. In: The Economist, 21 May 2016, 57.

World Economic Forum (2020): The Global Risks Report 2020. Cologne/Geneva: World Economic Forum.

Elkhan Nuriyev

Competing Regionalisms in the EU's Eastern Neighborhood: Geopolitical Risks, Challenges and Prospects



Elkhan Nuriyev
Brussels Energy Club

Abstract

In den Ländern der Östlichen Partnerschaft, zu der sechs postsowjetische Staaten mit sehr unterschiedlichen Kulturen gehören, die zu unterschiedlichen außerregionalen Einflusspolen tendieren, dient der „neue Regionalismus“ als ein Schritt hin zu globaleren und multilateralen Beziehungen. In diesem Artikel wird untersucht, wie sich konkurrierende Regionalismen in einer unruhigen Nachbarschaft darstellen, in der die Europäische Union, Russland und China unterschiedliche Ansätze für die Dynamik der regionalen Integration verfolgen. Der Artikel geht der Frage nach, wie sich diese Unterschiede auf die Länder der Östlichen Partnerschaft auswirken, und erläutert gleichzeitig die aktuelle Komplexität im Beziehungsgefüge EU-Russland-China. Der Beitrag unterstreicht, dass es dringend notwendig ist, ein neues kooperatives Verhältnis auszuarbeiten, das innerhalb eines vereinbarten multilateralen Regelwerks gebildet wird, das ein System fördern würde, in dem Moskau, Peking und Brüssel gleichermaßen Verantwortlichkeiten und Beschränkungen auferlegt werden würden. Ihre Fähigkeit zur konstruktiven Zusammenarbeit wird darüber entscheiden, ob die Östlichen Partner spürbare Fortschritte bei der Friedenskonsolidierung, der nachhaltigen Entwicklung und der erfolgreichen Integration in die Weltwirtschaft erzielen.

In the Eastern Partnership region, which comprises six post-Soviet countries with very different cultures that lean towards different extra-regional poles of influence, “new regionalism” serves as a step towards more global and multilateral relations. This article examines how competing regionalisms are presented in a turbulent neighborhood where the European Union, Russia and China have different approaches to dynamics of regional integration. It explores how these differences impact the Eastern Partnership countries, while explaining the current intricacies of the EU-Russia-China triangle. The paper argues that there is a strong need to work out a new cooperative relationship formed within an agreed multilateral framework of rules that would foster a system aimed at imposing responsibilities and restraints on Moscow, Beijing and Brussels. Their capacity for constructive cooperation will determine whether the Eastern partners make tangible progress on peace building, sustainable development and successful integration into the global economy.

Keywords: Competing regionalisms, Eastern Partnership, dynamics of regional integration, EU-Russia-China triangle

1 Introduction

The last two decades have seen the emergence of new regional cooperation initiatives, including the Russia-led Eurasian Economic Union (EAEU)¹, the European Union's Eastern Partnership (EaP)² and China's Belt and Road Initiative (BRI)³. Although these are all at various phases of implementation, each one of them seems to entail bigger geopolitical visions promoting competing ideas of regionalisms. The way in which these regionalist integration projects are currently evolving in Eurasia means that the post-Soviet states are straddling fault lines and choosing sides in the entire region. Many important challenges facing smaller regional countries have placed them at the juncture of those potential fault lines. This is especially true for the EaP nations, which still remain, to varying degrees, unstable, unreformed, and embroiled in conflicts.

The primary purpose of this article is to investigate the main characteristics of competing regionalisms by assessing key factors that define region-building strategies of the European Union (EU), Russia and China under the current global condition. To achieve this objective, the paper starts by introducing the idea of "new regionalism" as a global geopolitical change in the post-Cold War era, giving a brief overview of different perspectives on reshaping the Eastern Partnership region. This is followed by an analysis of the EU's promotion of regionalism in the Eastern neighborhood, particularly the EaP. The next two sections look into major regional integration projects launched by Russia and China, with a specific focus on the EAEU and the BRI respectively. The article concludes with a discussion of what may lie ahead, primarily making inferences about the likely impact of new geopolitical realities in the post-Covid-19 world on the long-heralded regional structures, and suggesting possible ways in which the EU, Russia and China could facilitate cooperative efforts aimed at helping the EaP countries to foster greater stability, lasting peace and economic prosperity in the entire region.

2 The Geopolitics of "New Regionalism": Competing European and Eurasian Perspectives

Regionalism, whether competitive or cooperative, is intimately connected with geopolitics as it seeks to create regional spaces, boundaries, concepts, identities, narratives and ideologies for a regional project.⁴ In the post-Cold War era, however, "new regionalism" is inextricably linked to new regional realities, geopolitical rivalries, protracted territorial conflicts, instabilities, wars, sanctions, economic decline, and security interests. This explains why the geopolitics of "new

1 The Eurasian Economic Union (EAEU), formally established in May 2014, currently comprises Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia. The EAEU was formed with the aim of fostering closer economic cooperation among member states.

2 The Eastern Partnership (EaP), officially launched in May 2009, is a joint policy initiative aimed at closer political association and economic integration between the EU and the six post-Soviet states of Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

3 The Belt and Road Initiative (BRI), formerly known as One Belt One Road, is a global development strategy adopted by the Chinese government in 2013 involving infrastructure development and investments in nearly 70 countries and international organizations. All six Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) are BRI participants on the basis of their approval of bilateral cooperation agreements with China.

4 For an interesting overview, see Neumann 2003: 160-178.

regionalism” in the post-Soviet territory looks very complicated. Yet interestingly enough, neo-regionalism and economic liberalization could lead to more geopolitical competition, while infrastructure connectivity seeks to reshuffle patterns of trade. Interactions between the EaP, the EAEU and the BRI are of greater interest in the wider regional context. What is at issue in fact is the shape of the triangular relationship between the EU, Russia and China, and its strategic implications for regional security in Eastern Europe, the South Caucasus and even far beyond.

The EaP and the EAEU are nevertheless presented as attempts at region-building strategies in the shared neighborhood. Both the EU and Russia consider the regional integration initiatives they promote as mutually exclusive with each other – economically as well as politically. Right from the outset, Brussels encouraged various Eastern neighbors to enter into closer links with the EU, whereas Moscow reoriented its policies towards extensive cooperation with China in the framework of the Shanghai Cooperation Organization (SCO), and with some post-Soviet states via the evolving EAEU. While the EU seeks greater engagement with the EaP region to transform it into an area of peace, stability and democracy, Russia strongly resists the Europeanization in its “near abroad.” The EaP countries therefore continue to struggle to find their way between competing European and Russian narratives.

The BRI, in turn, serves as a vehicle of China’s economic expansion. Chinese engagement helps diversify the EaP countries’ trade relations beyond their traditional markets, most notably the Russian market. For the six partner states of the EaP, competing regionalisms have opened up a space to manage Russia’s hegemonic aspirations and to enhance their relations with the EU and China. These post-Soviet nations have discovered real economic and political benefits that this so-called competitive regionalization is offering: a possibility to rely on several donors, instead of just one, improved security, and enhanced international status. Such a range of options has helped the Eastern partners to self-position themselves in the wider geopolitical context to resist external pressures, while ensuring their increased sovereignty and regime recognition by outside powers.

Interestingly, the EaP states have been capable of utilizing the regional integration initiatives in their favor. Limited involvement and selective engagement with the EAEU, the EaP and the BRI have enabled them to balance ambitions of Russia, the EU and China, and to reduce their impact to a minimum by playing them off against each other. Facing geopolitical challenges inherent in the competing region-building projects, the partner states have chosen to cooperate incrementally, but not fully integrate. By doing so, they have devised a skillful strategy which yields significant benefits in terms of negotiating power. As a result, their self-positioning has become key to enhancing their roles not only in regional affairs but also on the international scene.

From a geopolitical standpoint, Russia-EU competition is most likely a real contest between opposing value systems and ideologies. Integration policies in both the EU and Russia are built on the view that internal security challenges originate outside their borders. Russia generally regards closer regional integration with the EU as a geopolitical loss, while the EU views growing

rapprochement with Russia as an attempt to restrain its own regional leverage. Because the EU and the EAEU are in direct competition with each other, Brussels and Moscow are locked into a struggle over who is most capable of attracting the partner countries and under what terms and conditions. Given the impact of long-simmering conflicts in Nagorno-Karabakh, Abkhazia, South Ossetia, Transnistria and Donbas on the future EU cooperation policies towards the EaP countries, Moscow could exploit internal fault lines to serve as a major arbitrator in the peace process (Nuriyev 2019) and pursue its objectives through military tactics. As a consequence, Russia's geopolitical activism challenges strategic EU integration initiatives and creates dividing lines that could have broader geostrategic implications for Western democracies.

However, the challenge faced by Brussels in advancing a more integrated and effective policy in the Eastern neighborhood is not only an external one, but also internal as there are EU member states that still share relatively different views about the rationale, importance and ultimate goal of the EaP. The EU member states have not coordinated with each other to craft achievable policy goals, while Russia and China are strengthening their strategic cooperation, putting forward joint narratives and moving closer to creating their own Eurasian security alliance to compete actively against the West. Such a complex reality involves two competing European and Eurasian visions for reshaping the region, which prolongs the cycles of instability but does nothing to resolve regional security problems in the shared neighborhood.

3 Constraints and Shortcomings of EU-Steered Regionalism

Evidently, rapid improvements in relations between the EU and the post-Soviet states made in 2004 and 2009 were spurred by a series of new geopolitical breakthroughs such as the European Neighborhood Policy (ENP) and the EaP initiative. At that time, Eastern Europe and the South Caucasus became areas of direct concern to the EU strategy, which underwent an overall transformation from enlargement to regionalization. The EU opened a new chapter in multilateral cooperation with its Eastern neighbors (Council of the European Union 2009: 6), offering them privileged relationships based on mutual commitment to common values. While assuming a greater regional role through the ENP Action Plans, which were later replaced by Association Agreements, the EU has sought to persuade the post-Soviet leaders to adopt reform measures that would contribute to fostering stability and security. (Ferrero-Waldner 2020). Despite an expansionist regionalist logic of EU integration geared towards acquiring reliable partners (Headley 2012: 428), Brussels did not promise them eventual EU membership but rather sought to make the entire region more controllable and to create a secure geopolitical buffer between itself and Russia. It is therefore no surprise that since its launch the effectiveness of the EaP has been called into question. The critics have argued that the EU lacks the ability to offer its partner countries the full benefits of freedom, interaction and cooperation. (Christou 2010: 413-430; Wiśniewski 2013: 38)

In principle, two major factors have influenced the EaP's policy expectations in the EU's eastern periphery in recent years. Firstly, right from the outset the EaP required strong support from the EU member states that are still playing a key role in the formation of pan-European regionalism with the aim of integrating the post-Soviet states with the European Community. While some EU member states have failed to take an active stance, others simply lack a strong vision when it comes to reorientation of EU policy towards its Eastern neighborhood. Polarization within the EU between those that prefer to pursue a "Russia-first" policy and those that see it as the most serious obstacle to the formation of an effective strategy towards the Eastern neighbors has therefore impeded a recalibration of the EU's integration policy in this part of the world.

The second point is of even greater importance. The expectations of the partner countries regarding the EaP differ not only from that of the EU member states, but also from each other's. The countries are distinct in terms of their situations, resources and weaknesses. The EU has therefore sought to find ways of responding to the heterogeneity of the EaP nations, which are characterized by different degrees of interest in EU integration. The signing of Association Agreements,⁵ including Deep and Comprehensive Free Trade Areas (DCFTAs)⁶, with Georgia, Moldova and Ukraine certainly helped advance the EU's political and economic interests in the Eastern neighborhood, thus adding value to the ENP. The key question, however, is whether both the EU and the partner countries would succeed in committing themselves to meeting the EaP's policy goals in the years to come.

The EU has not been able to act coherently as a single state actor in devising a comprehensive strategy for the EaP region. This failure has limited the EU's influence and enabled Russia, via "smart power" diplomacy, to consolidate its geopolitical standing in the "near abroad" countries. Moreover, Russia's heavy military presence in the conflict-torn areas has complicated the EU's strategic thinking on Eastern Europe and the South Caucasus. Moscow can affect the security situation of the post-Soviet states in both positive and negative ways, whilst Brussels does not have such direct leverage since the EU has refused to become a relevant security actor. The very fact that Brussels lacks the necessary tools to intervene in the peace processes, offering instead only confidence-building activities, vividly testifies to the absence of a visionary and principled EU approach to resolving regional security issues. These constraints have raised questions about the adequacy of the EaP and hindered Brussels's capacity to formulate a meaningful policy to deal with simmering secessionist conflicts.

5 Georgia, Moldova and Ukraine signed their respective association agreements with the EU on 27 June 2014. These entered into force on 1 July 2016 in the case of Moldova and Georgia, and on 1 September 2017 in the case of Ukraine. On 24 November 2017, the EU and Armenia signed the comprehensive and enhanced partnership agreement, which entered into provisional application on 1 June 2018. Negotiations between the EU and Azerbaijan are still underway to conclude a new strategic cooperation agreement. Likewise, the bilateral relationship between Minsk and Brussels will be strengthened through the EU-Belarus Partnership Priorities, which are currently being negotiated.

6 DCFTAs, part of each country's EU Association Agreement, are free trade areas established between the EU and Georgia, Moldova, and Ukraine respectively. DCFTAs allow Georgia, Moldova and Ukraine access to the European Single Market in selected sectors and grant EU investors in those sectors the same regulatory environment in the associated country as in the EU.

Strikingly, none of the EU's member states are able to independently exert significant impact on the EaP nations caught in between European and Eurasian integration processes. If these Western European democracies acted in concert against Russia's new geopolitical self-confidence in the shared neighborhood, then the EU could probably become the most influential power in the medium to long-term. The incapability of the European powers to shape a common and well-integrated policy for the EaP region has prevented them from achieving their full potential. The EU's overall strategy has clearly been dominated mainly by considerations of how European policies will affect relations between Brussels and Moscow.

Overall, the EaP is most at risk if no concrete actions are taken on the part of the EU. Therefore, the EU's engagement with the EaP countries should be more intensive and assiduous than ever. Likewise, the EU should have a clear political risk mitigation strategy which can enable Brussels to produce effective responses to a range of potential risks. Comprehensive due diligence investigation, deep dive research, and political risk analysis are the most important foundational elements of such a strategy.

The EU has undoubtedly played a vital role in expanding strategic cooperation with its Eastern neighbors. At the same time, however, Brussels has completely failed to involve Moscow in its pan-European regional integration initiatives, with the Kremlin perceiving the EU-steered regionalism as encroaching on what Russia considers its natural sphere of influence. This has all ultimately damaged the interests of the Eastern partner states that are perpetually striving to counter undesirable foreign competition pressure and avoid possible unintended consequences.

4 Eurasian Economic Union: Motives for Russian Regional Hegemony

As Russia's President Vladimir Putin examines the real power situation in the international arena (Nuriyev 2018a), the significance of the post-Soviet territory becomes abundantly clear to the Russian Federation. Following the dissolution of the USSR, the Kremlin initiated the creation of several regional intergovernmental organizations, which began countering the EU's policy initiatives right from the outset, leading to what some scholars have called a "clash of integration processes." (Casier 2007: 73-94; Kanet/Freier 2012: 276). The most significant of these structures include the Commonwealth of Independent States (CIS), established in late 1991, the Collective Security Treaty Organization (CSTO), created in 2002, the Union State of Russia and Belarus, formally launched in 1996, and the Customs Union, which came into existence in 2010 and was then succeeded by the Eurasian Economic Union (EAEU) in 2015.

Internationally, the Kremlin advocates a geopolitical philosophy highlighting that the EU should accept Russian-style realpolitik and respect the rules of the game set by Moscow for the post-Soviet realm. In order to re-emerge as a great power, Russia is concentrating on expanding strategic ties with the CIS states, strongly insisting that its post-Soviet neighbors not only retain but also strengthen their security arrangements with Moscow. Eastern Europe, the South

Caucasus and Central Asia are hence three vital regions of critical national interest to Russia, which cannot simply shirk engagement there. In addition to promoting strategic initiatives within the scope of the CSTO and the SCO, Putin's EAEU project is a well thought-out plan and a current passionate manifestation of the logic of "protective integration." (Allison 2010: 29-48)

Territorial dimension matters significantly to Russia, which has exploited "new regionalism" not only to counter geopolitical expansion of the EU's influence but also to recover lost terrain. Russia threatened the CIS countries that were willing to enter into closer institutional and economic links with the EU with potential counter-reactions to try to convince them to instead join the EAEU. Moscow clearly demonstrates its geopolitical vigor and frequently uses hardline methods to safeguard Russian national interests. While also using non-military tools of persuasion to convince countries to join the EAEU, the Kremlin has simultaneously taken a very confrontational anti-Western posture, leading to more clashes with Brussels and with several EaP countries that have adopted a pro-Western course. The inability of Moscow and Brussels to shape their bilateral relations in a mutually beneficial way has resulted in a competition of regionalisms and increased mutual distrust. This reflects the emergence of a dangerous fault line separating two civilizations in the shared neighborhood, because the intense rivalry between the EU-sponsored EaP and the Russia-driven EAEU represents a civilizational choice.

In essence, Russian policymakers believe that the process of westernization represents an obvious threat to Russia's national security. (Nygren 2008; Green 2012). The very fact that European policies are backing Western economic goals for the wider Black Sea-Caspian basin has already brought the EU into conflict with Russia's strategic interests. The issues of pipeline routes, foreign policy trade-offs, and regional security likewise tend to involve intense competition over who receives how much gas. With Russia's geopolitical assertiveness growing in the entire region, there is also much talk in Moscow about the need to protect the country's frontiers and turn them into an impenetrable barrier against would-be adversaries of the Russian state.⁷

The security dynamics in the post-Soviet space are becoming increasingly relevant due to the EaP countries' relations with Russia, which actively pursues regional integration with a view to securing regional hegemony. As all six EaP countries face complex domestic processes inevitably affecting the security of Russia itself, the Kremlin's mediating role in the region is firmly rooted in common security interests. Because of its capabilities and reach, Moscow can further enhance its geopolitical clout in various, subtle ways so as to orchestrate conflict settlement scenarios that will not only serve Russian strategic interests but also in the end gratify Armenia, Azerbaijan, Georgia, Moldova and possibly Ukraine. The Kremlin seems to be waiting for a suitable time and favorable circumstances before placing Russia's weight behind a solution to regional security issues. This puts Moscow in a position of power as the central arbiter of a future peace settlement, but it also reinforces Russian responsibility if something

⁷ Author's private discussions with Russian experts who requested anonymity, Moscow, 17 October 2009 and 19 May 2015.

goes wrong. It remains to be seen, however, whether Russia can eventually turn these obstacles into opportunities.

Russia is certainly a powerful regional neighbor with genuine security concerns in the CIS countries and will remain so in the future. President Putin has described Russia as “not just a country but a distinct civilization.” (Klishin 2020; Tsygankov 2016: 145-158). It is no surprise, then, that the Kremlin has a strong desire to recreate the former Soviet territory with a new outlook, mainly arguing that “Eurasian integration is a chance for the entire post-Soviet space to become an independent center for global development, rather than remaining on the outskirts of Europe and Asia.” (Putin 2013). As one Moscow-based policy analyst points out, it is not imperial ambition that lies at the heart of this policy, but rather Russia’s security needs, whereby the Russian policymaking process is defined by the best way to maintain security.⁸ Such a regional perspective best illustrates Russia’s broad interests, of which Putin’s Eurasian Union is but one important part.

It is commonplace among Western scholars to define Russia as a revisionist power (Krastev 2014)⁹. Yet the character of Russia’s revisionism, including whether it adopts neo-imperial forms, is largely shaped by foreign and domestic influences. Some experts in Moscow have therefore called Russia a “restorative power” seeking to reclaim what it believes is rightfully its own.¹⁰ The restoration of the status quo ante implies a reversion to colonial boundaries. This is exactly why Putin famously said in a recent interview that former Soviet republics had left the USSR in 1991 together with “a huge amount of traditional historically Russian land.” (Putin 2020; Popovych/Lubkivsky 2020). Although his spokesperson later rebutted territorial claims on ex-Soviet nations, Putin’s statement seems to have questioned the redrawn borders of Russia after the collapse of the Soviet Union. (RFE/RL’s 2020). This vividly suggests that the Kremlin leader has indeed revised the post-Cold War security order to something Russia sees as more favorable to her geostrategic goals. This likewise means that it is not merely Russia’s smart power at work that has been expanded through the EAEU as its institutional mechanism, but also its regional hegemony.

Nevertheless, while assessing prospects for Eurasian integration, Moscow makes strategic decisions that advance the Russian agenda of geopolitical influence and economic cooperation in the CIS space. In order to succeed with the EAEU and become a center of regional integration, however, Russia should first modernize itself and demonstrate its potential for long-term stability at any cost. Only by doing so can Moscow boost the Eurasian Union’s attractiveness for the EaP countries. This is why the next several years will prove decisive in the struggle to reshape the post-Soviet neighborhood and integrate partner states into Russia’s regional hegemonic project.

8 Author’s private conversation with a Russian political scientist who requested anonymity, Moscow, 6 May 2018.

9 For an alternative viewpoint, see also Loukianov 2015: 11-24.

10 Author’s private conversations with Russian political scientists who requested anonymity, Moscow, 15 May 2016.

5 China's Belt and Road Initiative: Ambitions and Realities

Another important player in the EaP region is China, whose growing global role has become increasingly apparent in the emerging new world order. Given their strategic position at the crossroads of Eurasian routes, Eastern Europe and the South Caucasus have particularly captured China's attention since the end of 2013, when President Xi Jinping proposed the concept of the BRI to revive economic, cultural and political exchanges along the ancient Silk Road (The World Bank.¹¹ While laying the foundations for a long-term presence in post-Soviet territory, China in recent years has cultivated closer relations with the EaP states and has presented itself to them as a crucial trade partner that engages impartially with all participating nations, including those in conflict with one another.¹²

As Beijing fosters ties with regional elites, Chinese companies have become very active, investing in port terminals and transport infrastructure, and more projects are underway that are consistent with intensifying cooperation in a variety of fields. For example, in Belarus, which benefits from closeness to the European market, China has created an industrial park that is intended to support joint production and logistics hubs. Chinese Shipping Group has also launched container services in Moldova's main port, Giurgiulesti on the Danube River. Moreover, Beijing is stimulating local investments in support of the creation of new freight corridors such as the Trans-Caspian International Transport Route (TITR),¹³ which connects Europe with Kazakhstan and China through the South Caucasus and the Caspian Sea. This route has already enabled trains operated by Kiev to bypass Russia's transit ban on Ukrainian goods by shipping cargo through the Black Sea, Georgia, and Azerbaijan.

Although Beijing rarely pursues a political agenda openly, Chinese leadership appears to be rather open to negotiating with incumbent leaders and providing them with financial support in exchange for economic benefits. While engaging with the entire region, China pursues quiet diplomacy aimed at discovering all of the possible avenues which best serve its interests. Even if Chinese presence remains modest compared to that of Russia and the EU, Beijing's model of integration based on its intense promotion of the BRI, complete with big promises to invest in many different sectors, is seen as a "new option" (Denver 2017) able to help the EaP countries increase their involvement in global commerce and reduce their respective economic vulnerabilities as well as improve their infrastructure and boost their economic growth.

Clearly, an extension of Beijing's economic influence could increase Chinese investments to further enhance regional development. The key question, however, hinges upon whether the promises of these investments will be fulfilled. Despite interest from Beijing in the infrastructure

11 For more details, see The World Bank, Belt and Road Initiative <https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative>.

12 On several occasions China has tried to remain neutral over secessionist conflicts in the post-Soviet space. In particular, Beijing abstained during the 2008 vote about Armenian-Azerbaijani conflict over Nagorno-Karabakh in the UN Security Council and did not take a position over Russia's conflict with Georgia in the same year, nor over Russia's conflict with Ukraine in 2014.

13 TITR is also called a "middle corridor" in the BRI project. For more on this issue, see <https://middlecorridor.com/en>

projects connecting China with Europe, a sound basis for its greater strategic engagement with the EaP nations has yet to be formed. Beijing does not seem to have a clear vision for materializing the BRI in post-Soviet territory.¹⁴ Indeed, the reality of China's investment flows into the EaP states does not match official rhetoric. Most BRI-related joint activities remain in the planning phase and it is still unknown whether investment projects will actually be implemented.

Meanwhile, the BRI is perceived in wider geopolitical terms, especially when taking into account that China-steered regionalism promotes a new vision of Asian geo-economic order aimed at integrating beyond the borderlines of the nation-states. Examining the EU's and Russia's perspectives on the BRI's current status and outlook in their shared neighborhood is of greater interest here. There is a strong connection between China's increased economic involvement in the EaP region and Beijing's relations with Moscow. China is at times ambivalent towards regionalization of the emerging market economies, and at times unable to foster stronger regional ties because pure economic power is not sufficient to do so. Possible answers include geopolitical considerations of post-Soviet elites, which drive them closer to Russia, and the weakness of China's civilizational rhetoric which is insufficient to promote Chinese norms and values in the EaP countries. China-Russia relations are therefore crucial to understanding the nature of their impact on regional cooperation.

At present there is an ongoing profitable convergence of strategic Sino-Russian interests. China seems to have implicitly recognized Russia's privileged position in post-Soviet Eurasia. (Dias-Fernandes/Ageeva 2020: 523-540). In response, Russia has recognized the positive potential of the BRI and is increasingly accepting a conciliatory approach to China's vigorous push in the EaP region, particularly following Western sanctions, which has led to Moscow's greater dependence on Beijing. This is, however, more due to strategic compulsions rather than a conscious choice. For Russia, the BRI is conducive to the creation of a multipolar world as it bolsters China's global stance in relation to counterbalancing American hegemony. Russia also views the BRI as a means to attract Chinese investment in its economy and perhaps most critically, as a source of significant transit revenues from trans-Eurasian rail freight.

At the same time, the EAEU and the BRI appear to be more complimentary than mutually exclusive. A major goal of the BRI is to merge with the EAEU¹⁵, which gives Russia a competitive advantage in trans-Eurasian land-based transit because freight traversing the EAEU must pass customs only once between China and the EU. To take greater advantage of trans-Eurasian freight routes under the BRI, Russia is supporting efforts towards regulatory convergence and soft infrastructure development in Eurasia. Moscow is also working to promote coordination

14 Some of the Chinese experts themselves acknowledge that their country lacks the institutional capacity to manage the financial and reputational risks that the BRI entails. These are personal views expressed by two Chinese political scientists with whom the author had private conversations at the international conferences held in Minsk, Tbilisi and Zurich during 2016-2017.

15 Interestingly, the Shanghai Cooperation Organization (SCO) is set to showcase alignment between China and Russia through integration of Beijing marshalled Silk Road Economic Belt and Moscow driven EAEU. For an interesting discussion of how the SCO, the BRI and the EAEU may create synergy, see John Joshua, *The Belt and Road Initiative and the Global Economy*, London: Palgrave Macmillan, (2019): 219 pp.

between multilateral institutions to make stable, long-term financing available for the BRI's capital-intensive components. However, the implementation of the EAEU and the BRI could trigger future geo-economic and geopolitical competition between Moscow and Beijing.

The EU, in turn, views the BRI in its Eastern neighborhood neither negatively nor unconditionally positively. The BRI's two economic corridors in Central Asia and the South Caucasus complement Brussels' vision of trans-Eurasian connectivity, though they are not coordinated with the EU. While highlighting opportunities and challenges for the European transport system (Steer Davies Gleave 2018: 118), Brussels also emphasizes weaknesses of these corridors, arguing that the New Eurasian Land Bridge is economically feasible but geopolitically hazardous in the context of the current alienation between the EU and Russia, whereas the China-Central Asia-West Asia Economic Corridor is more expensive but geopolitically safe. Both corridors, however, account for a tiny share of total EU-China trade.

Furthermore, China may enter into competition with the EU for access to Caspian energy resources. Chinese companies may be interested in buying Azerbaijani gas within the BRI if an agreement on laying a trans-Caspian gas pipeline is after all concluded between Turkmenistan and Azerbaijan. The BRI may thus bring economic growth and help consolidate the region's stability. But this will only occur if BRI-related projects do not undermine implementation of sustainable reforms promoted by the EU within the EaP policy. The EU needs to craft a new model of protective and cooperative integration. For this purpose, Brussels needs to have a radical rethink and should strongly support the creation of a new business and trade alliance, a unique network of enterprises in the EaP region with the aim of simplifying and improving regional trade and connectivity. This implies that Eastern European companies should be given proper representation in EU business circles to promote their industrial, energy and trade related project ideas.

6 Conclusion

The reason why the emergence of "new regionalism" in post-Soviet territory has resulted in competing region-building projects is the failure of Brussels, Moscow and Beijing to devise a coherent strategic plan that focuses on an integrated, consistent approach and recognizes the shared interests of Russia, the EU, China, and the EaP countries. The Covid-19 pandemic creates a new landscape of potential risks to the Eastern neighbors, which are likely to be further sidelined, especially now, as the EU strives to develop a coordinated position internally and externally, in addition to its unsuccessful efforts to uphold a united stance on Russia. Therefore, the political and economic impact of Covid-19 in the EaP region will highlight even more the crucial roles Russia, the EU and China can play in promoting competing regionalist paths in the context of new, unfolding geopolitical realities.

As the geopolitical tug of war heats up in the (un)common neighborhood, the Eastern partners will remain isolated regardless of whether a particular country chooses this or that economic integrative project. The failure of the EU to become more proactive in EaP affairs demonstrates its inability to build international support around interests that are in competition with Russian ones. (Nuriyev 2018b: 165-178). For many post-Soviet states, however, there is no economic promise offered by Russia, which cannot offer anything but regional hegemony over its neighbors because her economy is not performing well enough for it to be attractive for closer economic integration.

Paradoxically, some authors have recently argued for neo-containment, implying a commitment to a new strategy of containment for Russia as a carefully calibrated response to the Russian strategic challenge (Larsen 2020: 4). In the post-Covid-19 world, however, Russia may easily turn into an “unsatisfied,” revisionist power, seeking to regulate pan-European security among other things. If the EU continues to contain Russia, or if Moscow tries again to rebuild an exclusive sphere of influence in the “near abroad,” this will result in a competitive course, if not a confrontation, that will last decades and may eventually put all regional integration initiatives in jeopardy. The strategic choices that the EU and Russia make today and particularly how they will act in the next few years to bridge potential fault lines will not only shape the contours of the emerging regional order, but also determine whether post-Soviet states Europeanize or stagnate. The solution to reconciling the EU and the EAEU, and hence breaking the isolation of the EaP countries, would be to establish free economic zones within them which were commercially accessible to either bloc, liberating Eastern partners from the painful consequences of their dilemma.

Concurrently, China’s geopolitical status is rapidly changing. Beijing’s growing influence in Europe has the potential to create new geo-economic divides, especially as Covid-19 has fostered anti-China sentiments already present within Western establishments. It is yet unclear how the set of BRI-related projects will be interconnected, as they depend mainly on expanding political relations with various EaP states pursuing different foreign policy goals. A key question hinges upon how Beijing will use political leverage gained through its BRI. Despite these uncertainties, the Chinese investment drive will remain eye-catching to the EaP countries because the BRI has the potential to significantly contribute to regional economic development.

Nevertheless, competing regionalism can be transformed into cooperative regionalism. The EU-Russia-China triangle may ultimately benefit from regional integration activities if Brussels, Moscow and Beijing can re-engage partner countries by opting for a positive sum strategy rather than a negative-sum game. This entails that the success of cooperative regionalism is linked to the ability of the three powerful actors to redefine their relationship and cooperate more constructively. The EU, Russia and China should think strategically about working out a new cooperative relationship formed within an agreed multilateral framework of rules that would foster a system aimed at imposing responsibilities and restraints on Moscow, Beijing and Brussels. Their capacity for constructive cooperation will determine whether the EaP

countries can make tangible progress on peace building, sustainable development and successful integration into the global economy.

7 References

Allison, Roy (2010): Virtual Regionalism and Protective Integration in Central Asia. In: Sengupta A. / Chatterjee S. (eds.): Eurasian Perspectives: In Search of Alternatives. Delhi: Shipra Publications, 29-48.

Casier, Tom (2007): The Clash of Integration Processes? The Shadow Effect of the Enlarged EU on Its Eastern Neighbours. In: Malfliet K. / Verpoest K. / Vinokurov E. (eds.): The CIS, the EU and Russia: Challenges of Integration. Basingstone: Palgrave Macmillan, 73-94.

Christou, George (2010): European Union Security Logics to the East: the European Neighborhood Policy and the Eastern Partnership. In: European Security, 19(3), 413-430.

Council of the European Union (2009): Joint Declaration of the Prague Eastern Partnership Summit. Prague, 7 May 2009. 8435/09 (Presse 78), 6.

Denyer, Simon (2017): Move Over, America. China Now Presents Itself as the Model 'Blazing a New Trail' for the World. In: The Washington Post, 19 October 2017.

Dias Fernandes, Sandra / Ageeva, Vera (2020): Facing China in Eurasia: The Russian Perspective. In: Leandro F. / Duarte P. (eds.): The Belt and Road Initiative. Singapore: Palgrave Macmillan, 523-540.

Ferrero-Waldner, Benita (2009): Eastern Partnership – An Ambitious Project for 21st Century European Foreign Policy. Statement by European Commissioner for External Relations and European Neighbourhood Policy on the Eastern Partnership. European External Action Service. Brussels, 20 February 2009.

Greene, James (2012): Russian Responses to NATO and EU Enlargement and Outreach.' London: Chatham House Briefing Paper.

Headley, James (2012): Is Russia Out of Step with European Norms? Assessing Russia's Relationship to European Identity, Values and Norms Through the Issue of Self-Determination. In: *Europe-Asia Studies*, 64(3), 428.

Kanet, Roger / Freier, Maria (eds.) (2012): Competing for Influence: The EU and Russia in Post-Soviet Eurasia. Dordrecht: Republic of Letters Publishing, 276.

Klishin, Ilya (2020): Putin and the ‚Distinct Russian Civilization‘. In: The Moscow Times, 25 May 2020. <https://www.themoscowtimes.com/2020/05/25/putin-and-the-distinct-russian-civilization-a70370>

Krastev, Ivan (2014): Russian Revisionism. In: Foreign Affairs, 3 March 2014. <https://www.foreignaffairs.com/articles/russia-fsu/2014-03-03/russian-revisionism>

Larsen, Henrik (2020): Neo-Containment: A Strategy toward Russia. In: CSS Policy Perspectives, 8(1), 4.

Loukianov, Fiodor (2015): Russia, a Revisionist Power?. In: Politique étrangère, Issue 2, 11-24.

Neumann, Iver B. (2003): A Region-Building Approach. In: Söderbaum F. / Shaw T.M. (eds.): Theories of New Regionalism. London: Palgrave Macmillan, 160-178.

Nuriyev, Elkhan (2018a): Endless Endgame: Whither Russia-West Confrontation?. In: Russia in Global Affairs, 06.04.2018. <https://eng.globalaffairs.ru/authors/elkhan-nuriyev>

Nuriyev, Elkhan (2018b): Russia-West Confrontation and the Future of European Security: Global Trends and Regional Consequences. In: Labarre F. / Niculescu G. (eds.): What a ‚New European Security Deal‘ Could Mean for the South Caucasus. Vienna: Austrian National Defence Academy, 165-178.

Nuriyev, Elkhan (2019): Peace building in the Eastern Partnership: What Roles for Russia and the EU?. In: ZOiS Spotlight, 45/2019, <https://en.zois-berlin.de/publications/zois-spotlight-2019/peace-building-in-the-eastern-partnership-what-roles-for-russia-and-the-eu>.

Nygren, Bertil (2008): The Rebuilding of Greater Russia: Putin’s Foreign Policy towards the CIS Countries. London/New York: Routledge.

Popovych, Nataliia / Danylo Lubkivsky (2020): Czar Putin Wants a New Age of Empires. In: Atlantic Council, UkraineAlert, 6 July 2020. <https://www.atlanticcouncil.org/blogs/ukrainealert/czar-putin-wants-a-new-age-of-empires>.

Putin, Vladimir (2013): Speech before members of the Valdai International Discussion Club. Moscow, Russian Federation, 20 September 2013. https://valdaiclub.com/a/highlights/vladimir_putin_meets_with_members_the_valdai_international_discussion_club_transcript_of_the_speech_/?sphrase_id=701234.

Putin, Vladimir (2020): Gifts from the Russian People. In: Russia-1 TV, 21 June 2020, Original comments (in Russian) are available at <https://www.youtube.com/watch?v=GcNEb9VZvzw&feature=youtu.be>.

RFE/RL's Russian Service (2020): Kremlin Denies Eyeing Territorial Claims After Putin's Comments in Documentary. In: RadioFreeEurope RadioLiberty, 22.06.2020. <https://www.rferl.org/a/kremlin-denies-eyeing-territorial-claims-after-putin-s-comments-in-documentary/30684797.html>.

Steer Davies Gleave (2018): Research for TRAN Committee: The New Silk Route – Opportunities and Challenges for EU Transport (Study). European Parliament, Directorate-General for Internal Policies, Policy Department for Structural and Cohesion Policies, 118. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/585907/IPOL_STU\(2018\)585907_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/585907/IPOL_STU(2018)585907_EN.pdf).

The World Bank (2018): Belt and Road Initiative, 29.03.2018. <https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative>

Tsygankov, Andrei (2016): Crafting the State-Civilization: Vladimir Putin's Turn to Distinct Values. In: Problems of Post-Communism, 63(3), 145-158.

Wiśniewski, Paweł Dariusz (2013): The Eastern Partnership – It is High Time to Start a Real 'Partnership.' Washington: Carnegie Endowment for International Peace, 38.

Verzeichnis der AutorInnen

Dr. Beat Habegger

Beat Habegger ist seit 2011 Head Political Risk bei Swiss Re. Nach seinem Studium an der Universität St. Gallen und Sciences Po Paris arbeitete er als Risiko und Sicherheitsberater in einer privaten Unternehmung, war Projektleiter am Center for Security Studies der ETH Zürich und wissenschaftlicher Mitarbeiter bei mehreren internationalen Organisationen. Seit 2005 ist er zudem Lehrbeauftragter an der Universität St. Gallen.

Mag. Dr. Johannes Leitner, MA

Johannes Leitner leitet seit 2012 das Kompetenzzentrum Schwarzmeerregion an der Fachhochschule des BFI Wien. Seine Forschungsschwerpunkte und Expertisen sind Politisches Risiko Management, sowie formale und informelle Institutionen und deren Konsequenzen für internationale Unternehmen mit Fokus auf den postsowjetischen Raum sowie die Türkei. Johannes Leitner lehrte an Universitäten in Albanien, Deutschland, Finnland, Frankreich, Rumänien, Russland, Tschechien und Türkei. In zahlreichen Projekten mit Forschungsaufhalten in der Region analysiert er die regimespezifischen politischen Risikofaktoren und deren Auswirkungen auf Unternehmen. Die Ergebnisse sind in wissenschaftlichen Zeitschriften, und Büchern publiziert. Johannes Leitner war zuvor Unternehmensberater und von 2005 bis 2010 Assistent an der Wirtschaftsuniversität-Wien mit Forschungsaufenthalt an der Stockholm School of Economics. Johannes Leitner hat an der WU-Wien und in Italien Internationale Betriebswirtschaft studiert; einen Master in South-East-European Studies an der Universität Wien und ein Doktorat an der WU-Wien absolviert.

Dipl.-Pol. Dr. Hannes Meißner

Hannes Meißner ist Senior Researcher und Lektor im Kompetenzzentrum Schwarzmeerregion. Seine Forschungsschwerpunkte sind Informelle Aspekte von Herrschaft, Politisches Risiko, Post-Sowjetische Transformationsprozesse, der „Ressourcenfluch“ und Governance-Initiativen.

2012 erlangte er den Doktor der Politikwissenschaft mit der Auszeichnung „magna cum laude“ an der Universität Hamburg. Während seines Doktoratsstudiums (2007-2012) wirkte er im Forschungsprogramm „Gewalt und Sicherheit“ des German Institute of Global and Area Studies (GIGA) und im Doktoratsprogramm „Informelle Netzwerke, Korruption und politische Regime“ der Forschungsstelle Osteuropa der Universität Bremen mit. 2008 wurde ihm ein dreijähriges Vollstipendium der Konrad-Adenauer-Stiftung, finanziert vom deutschen Bundesministerium für Bildung und Forschung, gewährt. Neben seiner Tätigkeit im Kompetenzzentrum Schwarzmeerregion hält er Vorträge und Seminare an der Universität Wien, der Konrad-Adenauer Stiftung und der Österreichischen Orientgesellschaft. Des Weiteren gibt er Gastvorträge an internationalen Partnerhochschulen, wie der Beykoz School of Logistics in Istanbul, der JAMK University of

Applied Sciences in Jyväskylä und an der Southern Federal University Rostov na Donu. Gleichzeitig hat er eine langjährige Erfolgsbilanz in der Durchführung von Langzeit Feldstudien, wie in Aserbaidschan, Turkmenistan, Georgien, Großbritannien (2009-2011) und der Ukraine (2013) vorzuweisen.

David Morris, MBA

David Morris ist internationaler Consultant und Senior Expert für China, Ostasien, Australien und den Pazifik. Er hat eine Reihe von leitenden Beraterfunktionen im asiatisch-pazifischen Raum und in Europa inne, unter anderem bei der United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). In den letzten vier Jahren war David Morris Pacific Trade & Investment Commissioner in China mit Sitz in Peking. Er ist ehemaliger australischer Diplomat, Handels- und Investmentbeamter und hochrangiger politischer Berater mit besonderer Expertise in Ostasien, Australien und dem Pazifik. 2018 wurde er zum Vizepräsidenten des ESCAP Asia Pacific Sustainable Business Network der Vereinten Nationen gewählt. Er wurde außerdem zum Vorsitzenden des United Nations Asia Pacific Business Forum 2019 ernannt, dem Flaggschiff der UN ESCAP-Businessesvents für den asiatisch-pazifischen Raum.

Dr. Elkhan Nuriyev

Elkhan Nuriyev ist Senior Experte für Russland, Osteuropa & Zentralasien und anerkannter Politikwissenschaftler mit einer starken Erfolgsbilanz in der politischen Analyse von Sicherheits- und Energiefragen in Russland, der Gemeinschaft Unabhängiger Staaten (GUS), der Eurasischen Region und der Region des Kaspischen Meeres. Er hat umfassende Kommentare, Briefings und Analysen für internationale Organisationen, Think Tanks, Regierungsbehörden und Unternehmen zur Verfügung gestellt. Als Alumnus der Russischen Akademie der Wissenschaften bekleidete er Regierungsposten in Aserbaidschan und eine Reihe von Gaststipendien in den USA und Deutschland, unter anderem an der George Washington University, dem Monterey Institute of International Studies, dem Woodrow Wilson International Center for Scholars, dem Deutschen Institut für Internationale und Sicherheitsfragen und dem Deutschen Rat für Auswärtige Beziehungen. Er ist Global Energy Associate beim Brussels Energy Club.

Working Papers und Studien der Fachhochschule des BFI Wien

2020 erschienene Titel Working Papers

Working Paper Series No 110

Michael Reiner: Der Report der High Level Group of Experts on Pensions der EU-Kommission: Impulse für die betriebliche Altersvorsorge in Österreich? Wien Dezember 2020

Working Paper Series No 111

Roland Schuster / Jürgen Radel: Dokumentation des Teaching Labs zum Lehrveranstaltungstyp Projektarbeit. Wien Dezember 2020

2019 erschienene Titel Working Papers

Working Paper Series No 105

Harun Pačić: Rechtsethik des Daoismus. Wien März 2019

Working Paper Series No 106

Harun Pačić: Katholische Rechtslehre: Der Codex Iuris Canonici aus dem Jahr 1983. Wien März 2019

Working Paper Series No 107

Harun Pačić: Vergleichende Rechtslehre: Einführung in die Grundlagen der Rechtsvergleichung. Wien März 2019

Working Paper Series No 108

Andreas Nachbagauer / Iris Schirl-Böck / Edgar Weiss: Erfahrungen und Übertragungsmöglichkeiten von Human-Factors-Praktiken für den Umgang mit Unerwartetem in komplexen Projekten. Wien April 2019

Working Paper Series No 109

Harun Pačić: Europäische Demokratie: Der (Unions-)Begriff der Demokratie als Inbegriff der menschengerechten Rechtsstaatlichkeit. Wien August 2019

2018 erschienene Titel Working Papers

Working Paper Series No 98

Michael Reiner / Robert Horvath: Das neue europäische private Altersvorsorgeprodukt PEPP (Pan European Personal Pension Product) und seine Marktgängigkeit im Binnenmarkt – Eine kritische Intervention. Wien Februar 2018

Working Paper Series No 99

Judith Brücker / Johannes Jäger / Andreas Nachbagauer: Regionale Headquarters lateinamerikanischer Multinationals in Wien. Wien April 2018

Working Paper Series No 100

Andreas Breinbauer / Sandra Eitler: Typologisierung der Headquarters in Wien im Hinblick auf die Nachhaltigkeit. Wien April 2018

Working Paper Series No 101

Johannes Leitner / Hannes Meissner: Politisches Risikomanagement aus der Perspektive österreichischer Managerinnen und Manager. Wien Mai 2018

Working Paper Series No 102

Andreas Nachbagauer / Iris Schirl-Böck / Edgar Weiss: Vom Umgang mit Unerwartetem – Human Factors-Praktiken für ProjektmanagerInnen. Wien Dezember 2018

Working Paper Series No 103

Nathalie Homlong / Elisabeth Springler: Impact of Chinese Multinationals on Global Labor Conditions and European Strategies. Wien Dezember 2018

Working Paper Series No 104

Andreas Breinbauer / Judith Brücker / Johannes Jäger / Andreas Nachbagauer: Emerging Market Multinationals in Europe – Implications for a Smart Location Policy. Wien Dezember 2018

2017 erschienene Titel**Working Papers****Working Paper Series No 93**

Andreas Nachbagauer / Barbara Waldhauser: Standortkriterien zur nachhaltigen Ansiedlung von regionalen Headquartern. Wien Juli 2017

Working Paper Series No 94

Andreas Beinbauer / Johannes Leitner / Katharina Becker: Identifikation und Best Practice Beispiele für eine nachhaltige Standortentwicklung. Wien Juli 2017

Working Paper Series No 95

Edgar Weiss: Was das Projektmanagement von der Human Factors Forschung lernen kann – Möglichkeiten der Übertragung. Wien September 2017

Working Paper Series No 96

Gerhard Ortner / Iris Schirl-Böck: Erfolgreiches Management von Unsicherheit in Projekten. Wien September 2017

Working Paper Series No 97

Andreas Nachbagauer: Management des Unerwarteten: Eine organisationstheoretische Sicht. Wien September 2017

2016 erschienene Titel**Working Papers****Working Paper Series No 88**

Roland Schuster: Essentials of the course „Organisational and Group Dynamics“, Writings on intervention science, (Degree Program SHRM, 3rd Semester). Wien Mai 2016

Working Paper Series No 89

Roman Anlanger / Wolfgang A. Engel / Roland J. Schuster: Gelebtes Corporate Social Responsibility in der Lehre. Wien August 2016

Working Paper Series No 90

Johannes Jäger / Bianca Bauer: Lateinamerikanische Multinationals und ihre Transnationalisierungsstrategien - Investitionspotenzial für Europa/Österreich/Wien. Wien August 2016

Working Paper Series No 91

Andreas Breinbauer / Johannes Leitner: Internationalisierungsstrategien und ADI-Dynamiken türkischer und russischer multinationaler Unternehmen mit Bezug auf Österreich/Wien. Wien August 2016

Working Paper Series No 92

Nathalie Homlong, Elisabeth Springler: Ökonomische Ansätze zur Erklärung der Attraktivität europäischer Staaten für chinesische Direktinvestitionen. Wien August 2016

Studien

Roman Anlanger / Wolfgang A. Engel / Roland J. Schuster / Gregor Weiche: Technischer Vertrieb Panelstudie 2016. Wien September 2016

2015 erschienene Titel**Working Papers****Working Paper Series No 85**

Nachbagauer Andreas: Charakterisierung eines Begriffes der sozioökonomischen Nachhaltigkeit für Headquarterstandorte. Wien April 2015

Working Paper Series No 86

Nachbagauer Andreas: Internationalisierungstheorien und sozioökonomische nachhaltige Entwicklung von Headquartern. Wien April 2015

Working Paper Series No 87

Johannes Jäger / Elisabeth Springler: Eigentumsstrukturen, grenzüberschreitende Investitionen und Entwicklungsdynamiken. Wien August 2015

Studien

Roman Anlanger / Wolfgang A. Engel / Roland J. Schuster: Technischer Vertrieb. Panelstudie 2015. Status quo des technischen Vertriebs. Wien Juni 2015

2014 erschienene Titel**Working Papers****Working Paper Series No 83**

Jäger Johannes / Mader Katharina / Springler Elisabeth: Zur Verknüpfung von postkeynesianischen und kritischen politökonomischen Perspektiven zur Analyse von Krisen. Wien Dezember 2014

Working Paper Series No 84

Jäger Johannes / Springler Elisabeth: Räumliche Rekonfiguration in Europa und Implikationen für Entwicklungsstrategien. Wien Dezember 2014

Studien

Roman Anlanger / Luis Barrantes / Wolfgang A. Engel / Roland J. Schuster / Gregor Weiche:
Technischer Vertrieb Panelstudie 2014. Wien Mai 2014

2013 erschienene Titel

Working Papers

Working Paper Series No 79

Karin Brännemann: The Strategic Importance of Intercultural Competency for Project Managers in the 21st Century. Wien Februar 2013

Working Paper Series No 80

Marcus Kliaras / Matthias Maurer: Spread Risk und Solvency II - Vergleich internes Modell vs. Standardansatz. Wien März 2013

Working Paper Series No 81

Patrick Burger / Marcus Kliaras: Jump Diffusion Models for Option Pricing vs. the Black Scholes Model. Wien Mai 2014

Working Paper Series No 82

Peter Sturm: Modelle, Normen und Methoden des Qualitätsmanagements und ihre Praktikabilität für die hochschulische Qualitätssicherung. Wien November 2013

2012 erschienene Titel

Working Papers

Working Paper Series No 68

Wolfgang Aussenegg / Christian Cech: A new copula approach for high-dimensional real world portfolios. Wien Jänner 2012

Working Paper Series No 69

Roland J. Schuster: Aus der Praxis für die Praxis: Didaktik Best Practice aus dem Studiengang TVM. Praxisbeispiele zum LV-Typ Projekt(arbeit). Wien März 2012

Working Paper Series No 70

Björn Weindorfer: QIS5: A review of the results for EEA Member States, Austria and Germany. Wien Mai 2012

Working Paper Series No 71

Björn Weindorfer: Governance under Solvency II. Wien August 2012

Working Paper Series No 72

Johannes Jäger: Solvency II. Eine politökonomische Perspektive auf die europäischen Regulierungen im Versicherungssektor. Wien August 2012

Working Paper Series No 73

Silvia Helmreich: Solvency II. Derzeitige und künftige Anforderungen an das Meldewesen der Versicherungen. Wien September 2012

Working Paper Series No 74

Christian Cech: Die Eigenmittelanforderungen an Versicherungen im Standardsatz von Solvency II. Wien September 2012

Working Paper Series No 75

Christian Steinlechner: Konzept zur Datenerhaltung für Forschungszwecke. Wien November 2012

Working Paper Series No 76

Alois Strobl: Immobilienindizes als Zeitreihe und als Funktion makroökonomischer Variablen. Wien November 2012

Working Paper Series No 77

Björn Weindorfer: A practical guide to the use of the chain-ladder method for determining technical provisions for outstanding reported claims in non-life insurance. Wien Oktober 2012

Working Paper Series No 78

Axel Zugschwert: Avatare und soziale Kompetenz von ProjektleiterInnen in globalen virtuellen Projektteams. Wien November 2012

Studien

Roman Anlanger / Luis Barrantes / Gerhard Karner: Vertriebscontrolling. Wissenschaftliche Studie 2012. Status quo des Vertriebscontrolling. Wien April 2012

Roland J. Schuster: Schriften zur Interventionswissenschaft. Organisationsform Hierarchie. Wien April 2012

Elisabeth Kreindl / Gerhard Ortner / Iris Schirl: Outsourcing von Projektmanagement-Aktivitäten. Wien März 2012

2011 erschienene Titel**Working Papers****Working Paper Series No 63**

Roland J. Schuster: Zur Methode der psychoanalytischen Organisationsbeobachtung. Wien Juli 2011

Working Paper Series No 64

Björn Weindorfer: Solvency II. Eine Übersicht. Wien August 2011

Working Paper Series No 65

Elisabeth Brunner-Sobanski: Internationalisierung und berufsbegleitendes Studieren. Wien August 2011

Working Paper Series No 66

Roland J. Schuster / Anton Holik / Edgar Weiss: Aus der Praxis für die Praxis – Didaktik Best Practice aus dem Studiengang TVM – Teamteaching. Wien Dezember 2011

Working Paper Series No 67

Grigori Feiguine: Versicherungswirtschaft in Russland. Chancen und Risiken der ausländischen Unternehmen auf dem russischen Versicherungsmarkt. Wien Dezember 2011

Studien

Elke Holzer / Rudolf Stickler: Die österreichische Versicherungswirtschaft. Struktur, Wirtschaftlichkeit und Entwicklung. Wien April 2011

Elisabeth Kreindl / Ina Pircher / Roland J. Schuster: Ein kritischer Blick auf die (Un)Tiefen des Begriffs *Kultur* im Projektmanagement. Wien Dezember 2011

**2010 erschienene Titel
Working Papers**

Working Paper Series No 58

Grigori Feiguine: Einflüsse der internationalen Finanzkrise auf den Finanzsektor Russlands. St. Petersburg 2010

Working Paper Series No 59

Johannes Jäger: Bankenregulierung in der Krise. Wien April 2010

Working Paper Series No 60

Günter Strauch: Gibt es Zwilligskompetenzen? Untersuchung 2010 mit dem KODE® System. Wien September 2010

Working Paper Series No 61

Elisabeth Kreindl: Virtuelle Arbeitsumgebungen. Zukünftige Arbeitswelten von geographisch verteilten Projektteams? Wien Dezember 2010

Working Paper Series No 62

Ina Pircher: Motivationsfördernde Maßnahmen und Anreizsysteme für Projektpersonal an Hochschulen am Beispiel der Fachhochschule des BFI Wien. Wien Dezember 2010

Studien

Wolfgang A. Engel / Roman Anlanger / Thomas Benesch: Technischer Vertrieb. Panelstudie 2010. Status quo des technischen Vertriebs. Wien Mai 2010



FH

**Fachhochschule
des BFI Wien**
Wirtschaft
Management
Finance



Fachhochschule des BFI Wien Gesellschaft m.b.H.
A-1020 Wien, Wohlmutterstraße 22
Tel.: +43/1/720 12 86
Fax: +43/1/720 12 86-19
E-Mail: info@fh-vie.ac.at
www.fh-vie.ac.at

ISBN 978-3-902624-60-4

