Remote assessment of countries' nuclear, biological, and cyber capabilities: joint motivation and latent capability approach

William Frankenstein [1,*]

Phone (412) 268-2670
Email frankenstein@cmu.edu

Ghita Mezzour [2]

Email mezzour@cmu.edu

Kathleen M. Carley [3]

Email kathleen.carley@cs.cmu.edu

L. Richard Carley [2]

Email: carley@ece.cmu.edu

[1] Department of Engineering and Public Policy, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA, 15213 USA

[2] Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, 15213 USA

[3] Center for Computational Analysis of Social and Organizational Systems, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 15213 USA

Abstract

Nuclear, biological, and cyber weapons are major components of national security policy. We currently rely on case studies of individual threats to understand the international distribution of latent capabilities of weapons

of mass destruction (WMD)—and typically look exclusively at commercial activity, scientific activity, or policy activity, without considering how these activities relate to other capabilities. Part of the problem of relying on these case studies is that the most interesting cases tend to be the outliers—making it difficult to generalize policy. Many of these case studies also ignore the threat of multiple weapons of mass destruction—the analyses focus exclusively on nuclear issues, biological issues, or cyber issues. We adapt Friedkin's socio-cultural model of influence and group dynamics to illustrate how countries are motivated to develop WMD using data on international hostilities, alliances, and expert opinion. We assess latent capabilities based on a country's scientific, commercial, and policy activity. After applying this approach, we develop a risk threat score for the country's nuclear, biological, and cyber capability, and use *k*-means to assess global trends and profiles in WMD development. By using this approach, we systematically consider all countries and do a joint analysis across the different technologies. We find that there are four broad profiles of countries: countries that invest heavily across all three technologies, countries that are invested in nuclear and cyber capability, countries that are solely invested in biological capability, and countries that are not invested in the three capabilities. These profiles provide a more holistic view of the threat landscape for policymakers.

AQ1

1. Introduction

Assessing countries' nuclear, biological, and cyber capabilities jointly is an important step in developing approaches to counter the threat posed by these capabilities. Once a country's weapons program is uncovered, the international community can collaborate to stall the program. Assessing such weapon capabilities is challenging due to the secrecy surrounding these programs and the dual-use nature of many of the technologies involved. Most prior work on capabilities assessment consists of case studies of particular countries, which tend to focus on individual technologies. While case studies provide in-depth analyses of individual country-level security decisions, such an approach runs the risk of not acknowledging other security motivations

posed by other types of weapons of mass destruction (WMD).

In this work, we compare approaches to systematically assess countries' capabilities to develop nuclear, biological, and cyber weapons. The approaches we consider examine all countries in the world and take into consideration both countries' motivations and latent capabilities. We assess motivations by modifying Friedkin's socio-cultural model of social influence and group dynamics to capture factors that motivate countries to seek such capabilities. This model is known as Friedkin's social influence model (Friedkin 1998). Friedkin's model is an iterative linear model that estimates an actor's future beliefs as a function of their initial beliefs, and the social influence that others bring to bear on them through their social networks~~, the beliefs of these others,~~ and external factors. The social influence process leads actors to equilibrate to each other, and so alter their beliefs in the direction of the beliefs of those with whom they are strongly connected. This model, including variants of it (De Mesquita and Stokman 1994), has been widely used to predict changes in positions by individuals and groups on contentious issues and the adoption of new technology. Further, a variant of this model was previously used to examine changes in countries' postures to utilize nuclear weapons (Carley 2011). We extend this model to consider both positive and negative relations among the actors and instantiate the model using networks of international hostilities and international alliances, and set our initial values according to expert opinion. We assess latent capabilities based on factors such as research, commercial, and policy activities.

AQ2

AQ3

AQ4

AQ5

AQ6

In our motivation assessment, we develop two versions of Friedkin's social influence model: a naïve model that assumes that all three technologies are strategic weapons, and a sophisticated model, which takes on different assumptions for biological and cyber weapons. For nuclear weapons, in this security-driven model, countries are motivated to develop nuclear weapons if they are in conflict with a country that has nuclear weapons, and less

motivated to develop nuclear weapons if they are in alliance with a country that already possesses these weapons. This assumption is extended to biological and cyber weapons in the "naïve" model to illustrate how the dynamics play out if we consider biological and cyber weapons to be strategic. We then develop more sophisticated models that acknowledge the specificities of bioweapon and cyber capability proliferation. For example, in the sophisticated model, we do not assume that a country that possesses bioweapons provides reassurance to its allies.

After assessing countries' capabilities separately in each of the three areas, we examine countries' overall risk profile—the risk that these countries are both motivated and capable of developing WMD. More specifically, by considering three different capabilities simultaneously, we allow for a comprehensive view of the threats posed by the proliferation of these technologies and capabilities. We compute a country's risk score for a given weapon as the product of the country's motivation for that weapon as calculated using our modified Friedkin~~'s~~ social influence model and the country's latent capability for that weapon. We give these risk scores as input to a clustering algorithm to identify countries' overall risk profiles. We find four risk profiles: (1) countries that pose risk in the three areas, (2) countries that pose nuclear and cyber risk, but no ~~bio~~biological weapons risk, (3) countries that pose ~~bio~~biological weapons risk, but no nuclear or cyber risk, and (4) countries that pose little risk in the three areas.

The rest of the paper is organized as follows: we first provide background on factors that motivate countries to develop such weapons, and on technological requirements for developing such weapons in Sect. 2. We present our motivation assessment methodology, the modified Friedkin model, in Sect. 3, and our latent capabilities assessment methodology in Sect. 4. We discuss our results in Sect. 5, outline future work in Sect. 6, and conclude in Sect. 7. Table 1 highlights the primary discussion points for the sections beyond background literature.

Table 1

Section guide to concepts and models described in the paper

Section	Concept	Method	Theory	Input variables

III	Motivation assessment	Adapted Friedkin model	Deterrence	State-level alliance networks, hostility networks,
IV	Latent capability	Scoring based on national indicators	Technological development	State-level scientific research, commercial activity, and policy signals
V	Risk profiles	*k*-means	n/a	Motivation and latent capability

AQ7

2. Background

2.1. Motivational factors

2.1.1. Nuclear

Countries develop nuclear weapons for a variety of reasons, from concerns arising from security deficits to a commitment to norms and prestige surrounding nuclear weapons. This work broadly comes out of two literatures: nuclear deterrence and nuclear proliferation. Nuclear deterrence is traditionally contrasted with compellence—threats, as opposed to actions—and arguments for deterrence have focused on actions between two nuclear states as opposed to actions between non-nuclear and nuclear states. Nuclear proliferation is concerned with the spread of nuclear material and ultimately, nuclear weapons, outside of the existing international regime outlined by the non-proliferation treaty (NPT). Unlike deterrence, the proliferation literature examines both internal domestic motivations for developing weapons in addition to motivations driven by external actors.

The literature on nuclear deterrence remains broadly based in Cold War thinking as doctrine and policy developed in response to a world with bipolar nuclear powers. Traditionally connected with realist theory, deterrence is commonly accepted to have evolved over at least three “waves” (Jervis 1979): an initial wave, which explored the impact of nuclear weapons on world politics; to a second wave, which combined policy and theory; to a third wave, which highlighted empirical work. The second wave, which incorporated game theory models, such as the ‘Chicken Game’, led to

important insights about the nature of international relations, but did not contribute to direct policy implications: while it explained superpower relations, and framed broad strategic issues, it did not significantly contribute to smaller diplomatic and military efforts (Kaplan 1983; Trachtenberg 1991). The lack of empirical evidence made it difficult to evaluate claims made in deterrence literature (Adler 1992), which ~~helped and~~ lead to the third wave's emphasis of empirical work on risk taking, rewards, misperceptions, and bureaucratic politics (Jervis 1979; Huth 1999).

AQ8

Traditionally, deterrence requires actors who are rational, resolute, and credible—all traits that rogue actors, such as North Korea, may not consistently demonstrate (Smith 2006). An alternate angle, however, is that the presence and threat of any type of weapon of mass destruction make deterrence easier (Lebovic 2007)—threatening an actor, combined with the crystallization of the risk posed by a WMD to other actors, can make it easier to respond to threats (Morgan 2003; Nolan and Strauss 1997). Others have argued that the WMD threat makes it easier for rogue states to deter other actors, such as the United States, from involvement (Jervis 2003; Litwak 2007).

These external motivations for developing nuclear weapons are most commonly associated with a realist, or security-based approach to developing nuclear weapons—one that focuses on nations as actors in a state of anarchy (Waltz and Sagan 2002). There are two other major schools, which include domestic politics and constructivism (Sagan 1996). The domestic politics school, which focuses on the role of different domestic actors, argues that the nuclear capability of a country can emerge from disparate actor politics, including responding to a international institutions, political economic ambitions, and nuclear ambivalence (Dai 2007; Solingen 2007); (Abraham 2006). The constructivist school, which focuses on norms, argues that national leaders and identity play a major role in country motivations (Hymans 2006; Tannenwald 1999; Rublee 2009).

We will focus on the mechanics of the security model in developing our motivation model for nuclear weapons, which has broad support (Waltz and Sagan 2002). In the security model, a country that has a nuclear enemy

perceives a security deficit, and is thus motivated to acquire nuclear weapons (Waltz 2010). The country may also seek an alliance with a nuclear power that promises retaliation in case the country is attacked (Betts 1993; Davis 1993; Thayer 1995). Such alliance provides reassurance for the country and reduces its need for developing indigenous nuclear weapons.

2.1.2. Biological weapons

Bioweapon deterrence and proliferation theory is not as developed as nuclear proliferation theory, with motivations for BW often discussed in the same work as literature discussing BW latent capability. A major concern with BW proliferation is the relatively low cost and ease of purchasing BW capability, allowing states to potentially change regional power dynamics at a much lower cost than obtaining a nuclear capability (Horowitz and Narang 2014). We base most of our discussion on the work by Tucker (2000), who relates nuclear deterrence with in-kind biological weapons deterrence. The first type of incentive listed by Tucker is in-kind deterrence to balance regional strategic power. If a country acquires a BW capability, its enemy states may seek similar capability to fill the resulting security imbalance. The second major incentive is deterrence of nuclear weapons use. Some states may seek BW with the goal of deterring nuclear attacks against them, as summarized by Sagan (2000). This is particularly the case for states that lack the technical and financial infrastructure required to build nuclear weapons. Other incentives are tactical military use, pursuit of regional hegemony, sabotage and terrorism, and counterinsurgency and assassination.

2.1.3. Cyber

Cyber proliferation theory is even more limited than bioweapon proliferation. Traditional deterrence theory relies on threats meant to deter action by other countries. However, in the cyber context, it is difficult to identify the attacker, assure a response, and outline national responses to an attack: three core components of national nuclear deterrence strategies (Elliott 2011).

There are many levels to consider when it comes to national-level planning for strategic cyber responses: the intent of the attack, credibly identifying a national organization as the source of the attack, identifying the target as a

public or private target, and maintaining a response capability (Libicki 2009). We can conclude that a country is motivated to develop cyber capabilities if the country has an enemy who has such capabilities. It is, however, unreasonable to believe that countries perceive reassurance from an ally that has such capabilities. Handling occurring cyber attacks requires direct access to sensitive computer systems across a range of different industries. Countries may not even want their allies to gain access to their sensitive systems, and may prefer developing indigenous capabilities.

2.1.4. Latent capabilities

Developing an indigenous program that involves a nuclear weapon, a biological weapon, or cyber capabilities requires a significant amount of technical knowledge, and in the nuclear and biological case, a non-trivial amount of infrastructure. Most of the work done on the "supply side" of nuclear proliferation focuses on broad industrial capabilities (Montgomery and Sagan 2011), and does not take into account the different types of indicators available to researchers today using open access tools. Here, we are interested in overall risk—we are not interested in distinguishing between the intelligence concern of "ambiguity", whether a country seeks weapons, or "opacity", where a country is hiding facilities to disguise its true goal (Frankel 1991). We consider these latent capabilities from the perspective of technological development, and consider the contexts that these capabilities would be detected: research capacity, commercial capacity, and the policy environment.

Drawing on the "supply side" literature of nuclear proliferation, we identify three broad categories of technical capability needed to develop a weapon: the basic science and engineering, the weaponization of the technology, and the safeguards needed to protect workers during testing. If a country attempts to hide these activities, whether through ambiguity or opacity, activity in these areas will still be reflected through the organizational aspects of the organizations supporting these activities: sometimes these will be apparent through commercial activity, especially in the case where the capability is purchased, and sometimes these will be apparent through policy activities. Table 2 summarizes the relationship between the types of signals we should expect to see from the relevant part of the technological development process.

We score overall latent capabilities in Sect. 4.

Table 2

Signals for latent capability detection by technology development and contexts

	Signal contexts		
	Research	**Commercial**	**Policy**
Steps in technological development			
Basic research	Academic and industrial research outputs	Trade in equipment related to technology	Treaties governing trade of sensitive materials
Weaponization	Research in more specialized areas of related technologies	Sale of missiles, technologies that exploit vulnerabilities	Policies regarding use of technology as a weapon
Safeguards	Issuing new worker restrictions, developing new research facilities in isolated areas	E.g. Trade in vaccines, detection equipment	E.g. Biosecurity Science Laboratories

2.1.5. Nuclear

To help conceptualize “supply side” determinants, researchers have turned to assessing a country’s overall latent capability—the self-sufficiency of the country’s nuclear industry. In doing so, many of these assessments focus on broad industrialized capacity. This work was started by Meyer (1984) and later further developed by Stoll (1996), and then incorporated into the quantitative analysis of proliferation by Jo and Gartzke (2007). Examples of such indicators are uranium deposits, steel production, and vehicle and radio production—all commercial signals. In closer case study analyses, Kroenig (2010) finds that states receiving specialized nuclear assistance are more likely to develop nuclear weapons, and Fuhrmann (2009) finds that any type of assistance increases the probability of a country developing nuclear weapons. These case studies considered primarily commercial and policy signals in basic research and safeguard steps.

Three major technical reports—*Swords from Plowshares*, Harney, and a technical report from the Pacific Northwest National Laboratory (PNNL)—focus on key steps needed to develop an indigenous weapons program and the length of time involved in achieving a full capability (Wohlstetter 1979; Harney et al. 2006; Talbert et al. 2005). By focusing on timelines, these papers implicitly highlight the organizational challenges involved in developing the necessary national institutions involved in nuclear weapons production, but instead explicitly only focus on institutional outcomes, the nuclear weapons technology. Furthermore, the focus on timelines obscures the difficulty of obtaining sufficient fissile material and the broader question of defining a "full capability" (Sagan 2010; Hymans 2010). Looking at weaponization exclusively, as these studies did, does not take into account the policy and commercial contexts that would arise that significantly impede further progress in developing the associated technology.

AQ9

AQ10

2.1.6. Biological

For biological weapons, signal detection is significantly more difficult due to the extensive amount of dual-use technology and commercial trade. An Office of Technology Assessment report outlines the steps that a country interested in developing BW will likely take Office of Technology Assessment (1993). In basic research, the country will establish facilities, conduct research, and develop BW agents at a small scale. Weaponization entails scaling up development by developing delivery systems, producing BW agents at a large scale, and stockpiling agents. The country's safeguards will include developing vaccines and respiratory masks.

The majority of equipment and expertise required for developing BW are dual-use with civilian applications in the pharmaceutical and fermentation industries. A country with moderately sophisticated pharmaceutical or fermentation industries can relatively easily develop BW.

2.1.7. Cyber

Cyber weapons are extremely sophisticated malicious computer programs

such as worms and viruses. Creating such weapons requires extensive cyber security expertise, but very limited equipment. Such weapons may be developed in large collaborations between military units, intelligence units, and state-sponsored industries. The most famous cyber weapon is Stuxnet, which targeted the Iranian nuclear program. Stuxnet caused nuclear centrifuges to run faster than their normal speed and eventually destroyed some of these centrifuges. Other less known cyber weapons include Duqu, Flame, and Gauss.

Many countries have created cyber security troupes within their military. Some of these countries declare that the goal of such troupes is exclusively defensive, while others declare that such troupes have both a defensive and an offensive mission. A clear signal to expect would therefore be stated military policy regarding cyber capabilities.

3. Motivation assessment methodology

The previous section provided the background literature for our motivational models and latent capability assessments. In this section, we first explain the technical details behind the Friedkin model and then develop the naïve and sophisticated versions of our motivation assessment. We conclude this section with an overview of the parameters and data used for these models.

3.1. Friedkin model

The model of social influence presented by Friedkin is a well-respected model of how actors change their attitude over time. The Friedkin model stipulates that actors' attitudes at time *t* are a weighted sum of the external influence from other actors and the actors' initial motivations. The model also stipulates that external influence takes the form of a linear sum of other actors' attitudes. More formally, in a group of N actors, the Friedkin model is described by Eq. 1.

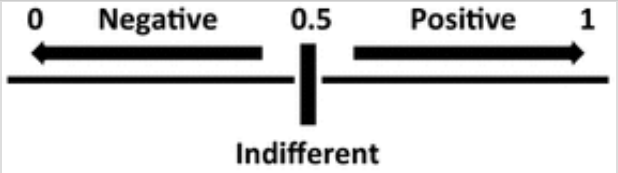
Equation 1: Friedkin model equation

$$y_t = AWy_{t-1} + (I - A)y_1 \quad 1$$

In the equation, y_t is an $N \times 1$ vector that represents actors' attitudes at time *t*. The attitude of each actor follows scaling given in Fig. 1, where 0.5 represents an indifferent attitude, larger values represent a positive attitude and smaller values represent a negative attitude.
$A = \text{diag}(a_{11}, \ldots, a_{ii}, \ldots, a_{NN}), 0 \leq a_{ii} \leq 1$ is a $N \times N$ diagonal matrix with diagonal weights indicating the level of influence that each actor puts on outside actors. $W = [w_{ij}], (0 \leq w_{ij} \leq 1, \sum_j^N w_{ij} = 1)$ is an $N \times N$ matrix that represent inter-actor influence. More specifically, w_{ij} represents the extent to which actor j has on actor i. *W* is computed using the formula $W = AC + I - A$, where $C = [c_{ij}]$ is a $N \times N$ matrix of relative interpersonal influence such that $(c_{ii} = 0, 0 \leq c_{ij} \leq 1, \sum_{j=1}^N c_{ij} = 1)$. Finally, y_1 is a $N \times 1$ vector representing actors' initial attitudes.

Fig. 1

Scaling of attitude values



At a high level, the Friedkin equation consists of three parts. Wy_{t-1} represents actors' extrinsic attitudes resulting from external influence, y_1 represents intrinsic attitudes that reflect actors' own characteristics and constraints, and *A* represents the relative weight that actors place on extrinsic and intrinsic attitudes. The Friedkin model can apply to any attitude. In this work, we consider the attitude to be the motivation to develop BW.

Unfortunately, the extrinsic attitude term Wy_{t-1} can only capture positive influence that results from friendly relationships. Thus, that term cannot capture both incentives and disincentives to developing capabilities. We develop each of the models in Sects. 3.3 and 3.4 by finding a new extrinsic attitude term that captures incentives and disincentives to developing the capability, and replacing Wy_{t-1} by the new extrinsic attitude term in the Friedkin equation.

3.2. Naïve models

The naïve model assumes that standard nuclear deterrence theory directly applies to bioweapons and cyber capabilities. We explain the naïve model in the context of nuclear weapons. The naïve models for bioweapons and cyber capabilities can be obtained by replacing “nuclear weapons” by “bioweapons” and “cyber capabilities” in the explanation below.

Standard nuclear deterrence theory stipulates that countries allied with nuclear powers may have disincentive to develop their own nuclear weapons (e.g. Germany and Japan), and that countries with nuclear rivals (e.g. India and Pakistan) may have incentive to develop nuclear weapons. Unfortunately, the Friedkin model equation can only account for influence in one direction, and thus cannot capture both incentives and disincentives. We slightly modify the Friedkin equation model to capture both positive and negative influence.

Friedkin’s equation captures extrinsic motivation, i.e. inter-state influence through Wy_{t-1}. Unfortunately, that term cannot capture both incentives and disincentives, and the interaction between incentives and disincentives. We find a new term that captures nuclear deterrence, nuclear reassurance, and the interaction between the deterrence and reassurance. We then substitute Wy_{t-1} in Eq. 1 by the new term to find the modified equation model. To simplify the discussion, we initially consider a single country that has a single enemy and a single ally, and derive a new expression capturing the extrinsic inter-state influence and motivation. Subsequently, we modify that expression into a vectorial expression that captures the extrinsic motivation of all countries. Finally, we include that vectorial expression into Eq. 1, obtaining the modified equation model.

We first codify the effect of incentives and disincentives on a country’s attitude toward developing nuclear weapons based on Table 3. In the table, nuclear enemy and nuclear ally indicate whether an enemy and an ally have nuclear weapons, respectively. When a country has a nuclear enemy and no nuclear ally, the country has maximum motivation to develop nuclear weapons. A nuclear ally provides reassurance, but the motivation remains positive as reassurance from an ally is never perfect. A country that has no nuclear enemy and no nuclear ally has absolutely no motivation for nuclear

weapons. Finally, a small motivation for nuclear weapons results from having a nuclear ally, but no nuclear enemy as the nuclear ally can provide nuclear assistance.

Table 3

Compiled effect of a nuclear enemy and a nuclear ally on country's extrinsic motivation to develop nuclear weapons

Nuclear enemy (e_{t-1})	Nuclear ally (f_{t-1})	Extrinsic motivation (m_t)
+1	+0	+1
+1	+1	+0.75
0	0	0
0	+1	+0.25

We find coefficients $\alpha_0, \alpha_1, \alpha_2$ and α_3 in Eq. 2 in order for the equation to satisfy conditions in the table above.

Equation 2: Extrinsic motivation coefficient equation

$$m_t = \alpha_0 + \alpha_1 e_{t-1} + \alpha_2 f_{t-1} + \alpha_3 e_{t-1} f_{t-1} \quad 2$$

Equation 3: Solved coefficients in extrinsic motivation equation

$$m_t = e_{t-1} + 0.25 f_{t-1} - 0.5 e_{t-1} f_{t-1} \quad 3$$

Equation 3 applies to only one country. We are interested in obtaining a vectorial expression that simultaneously captures the motivation of all states. We now assume that M_t, E_{t-1} and E_{t-1} are $N \times 1$ vectors. Equation 3 becomes

Equation 4: Vectorial form of extrinsic motivation

$$M_t = E_{t-1} + 0.25 F_{t-1} - 0.5 E_{t-1} \mathrm{diag}(F_{t-1}) \quad 4$$

Given that E_{t-1} captures whether countries' enemies have nuclear weapons at time t - 1, and F_{t-1} captures whether allies have nuclear weapons, we can write $E_{t-1} = W_H y_{(t-1)}$ and $F_{t-1} = W_F y_{(t-1)}$, where W_H captures international hostilities and W_F captures international alliances. Finally, we obtain

Equation 5: Naive model equation

$$y_t = A[W_{\mathrm{H}} y_{t-1} + 0.25 W_{\mathrm{F}} y_{t-1} - 0.5 W_{\mathrm{H}} y_{t-1} \operatorname{diag}(W_{\mathrm{F}} y_{t-1})] + (I - A) y_1 \quad 5$$

3.3. Sophisticated models

The naïve model captures standard nuclear proliferation theory, and is thus well suited for assessing countries' motivations to develop nuclear weapons. Unfortunately, nuclear proliferation theory does not directly apply to bioweapons and cyber capabilities. Thus, the naïve model is poorly suited for assessing countries' motivations for bioweapons and cyber capabilities. In this section, we explain how we modify the Friedkin model to capture factors that motivate countries to develop bioweapons in Sect. 3.3.1 and cyber capabilities in Sect. 3.3.2. We run an assessment of these newer models to demonstrate that the final results from these two types of models are different, and to highlight that changes in the assumptions used will result in distinct outcomes.

3.3.1. Bio-sophisticated model

We implement the bio-sophisticated model developed by Mezzour et al. (2014). In this section, we provide an overview of that model. The model explicitly captures in-kind deterrence, deterrence of nuclear enemy, and nuclear reassurance. The model implicitly captures other disincentives such as fear of international sanctions and uncertain military utility that arises out of the tactical use of biological weapons.

The bio-sophisticated model is developed using an approach similar to the one explained in Sect. 3.2. That is, a new extrinsic motivation term is

developed, and inserted into the Friedkin ~~equationin~~equation in the case of a single country that has a single enemy. Table 4 presents a qualitative description of a country's extrinsic motivation for BW as a function of the country's international environment. More specifically, the table examines three aspects of the country's international environment: (1) the enemy's ownership of BW, (2) the enemy's ownership of nuclear weapons, and (3) nuclear reassurance to the country. The country has nuclear reassurance when the country has nuclear weapons or is the military ally of a nuclear power. The country has high motivation for BW in case the country perceives a security deficit resulting from the enemy's ownership of nuclear weapons and/or BW, and the lack of nuclear reassurance. The country has moderate motivation for BW in case the enemy has BW and the country has nuclear reassurance. The country does not perceive a security deficit in this case, but may be interested in BW to be able to respond in kind. In the other cases, the country has low motivation for BW as there is no need for BW to deter BW use or nuclear weapon use.

Table 4

Qualitative description of the impact on a country's motivation to develop BW resulting from international influence

		Enemy has BW	**Enemy has no BW**
Country has no nuclear reassurance	Enemy has nuclear weapons	Very high	High
	Enemy has no nuclear weapons	Very high	Low
Country has nuclear reassurance	Enemy has nuclear weapons	Moderate	Low
	Enemy has no nuclear weapons	Moderate	Low

AQ11

In reality, countries are unsure about their enemies' BW programs due to the secrecy surrounding these programs. Therefore, it is more appropriate to model the enemy's ownership of BW as a continuous variable than as a

binary variable. Table 4 codifies the country's extrinsic motivation for BW as a function of the likelihood that the enemy has BW. The table assumes the likelihood that the enemy has BW is a continuous variable between 0 and 1 that has the scaling given in Fig. 1. The figure captures the fact that the country's motivation for BW increases as the certainty about the enemy's ownership of BW increases. The figure also captures the fact that the lack of nuclear reassurance and/or the enemy's ownership of nuclear weapons result in higher motivation for BW. Finally, when the country does not have nuclear reassurance and has a nuclear enemy, the marginal impact of the increase in likelihood is relatively low because the starting motivation is relatively high and the main driving incentive is the known enemy's nuclear weapons. It is worth noting the fact that the country's motivation for BW is always smaller than the likelihood that the enemy has BW implicitly captures disincentives and restraining influences such as uncertain military utility and the risk of provoking countermeasures.

AQ12

AQ13

Equation 6 is an expression of the country's extrinsic motivation for BW that satisfies the constraints in Table 5, where m_t is the country's extrinsic motivation at time *t*, b_{t-1} whether the enemy has BW at time $t-1$ that has the scaling shown in Fig. 1, c is whether the enemy has nuclear weapons and r is whether the country has nuclear reassurance.

Table 5

Table of effects for sophisticated ~~bio~~bioweapons model

Nuclear reassurance from ally	Nuclear enemy	Marginal impact of increase of likelihood of enemy having BW on country motivation	Starting motivation (when likelihood of enemy having BW is 0.5)
0	1	0.25	0.875
0	0	1	0.4
1	1	1	0.2
1	0	1	0.1

Equation 6: Expression of the extrinsic motivation of a single country to develop BW

$$\begin{aligned} m_t &= -0.1 + b_{t-1} + 0.85c - 0.3r - 0.75cb_{t-1} - 0.75cr + 0.75crb_{t-1} \quad 6 \\ &= (1 - 0.75c + 0.75cr)b_{t-1} + (-0.1 + 0.85c - 0.3r - 0.75cr) \end{aligned}$$

Equation 6 applies to only one country. We are interested in obtaining a vectorial expression that simultaneously captures the motivation of all countries. We now consider that M_t, B_{t-1}, C and R are $N \times 1$ vectors, where each value corresponds to one country, and we obtain Eq. 7.

Equation 7: Vectorial expression of all countries' extrinsic motivations to develop BW

$$M_{(t)} = \text{diag}[1 - 0.75R + 0.75\,\text{diag}[C].R]B_{(t-1)} - 0.1 + 0.85C - 0.3R - 0.75$$

Given that B_{t-1} captures whether states' enemies have BW at time $t-1$, we can write $B_{t-1} = W_H y_{(t-1)}$, where W_H is computed based on the hostility matrix. The bio-sophisticated model equation is thus given in Eq. 8.

Equation 8: Bio-sophisticated model equation

$$y_t = A(\text{diag}[1 - 0.75C + 0.75\,\text{diag}[C].R]W_H y_{t-1} - 0.1 + 0.85C - 0.3R - 0.7$$

In summary, the motivational change described in the sophisticated model can be described as a linear function: when the likelihood of an enemy having biological weapons increases, the motivation for the country to develop biological weapons goes up correspondingly. The functions for each potential case are shown in Table 5. In the case where the country does not have nuclear reassurance and has a nuclear enemy, the marginal impact of the increase in likelihood is relatively low because the starting motivation is relatively high and the main driving incentive is the enemy's nuclear weapons. As in the naïve model, it is important to remember that the impact

on motivation is a cumulative impact that is assessed simultaneously over all of a country's allies and enemies, and that a motivation of 0.5 indicates a country's indifference to developing biological weapons.

3.3.2. Cyber-sophisticated model

We only capture in-kind deterrence when modeling countries' motivations to develop cyber capabilities—the motivation that countries have to develop offensive cyber programs. Since we only capture motivation in one direction, we can directly use the Friedkin model equation, where W_H is computed based on the hostility matrix. The cyber-sophisticated model equation is thus given in Eq. 9. As there is no countering force in this model, we limit our analysis to the outputs of this model after 20 runs to identify the countries most impacted by cyber issues.

It is important to highlight a key difference between traditional deterrence theory and cyber operations: in a cyber event, it can be difficult to credibly identify the source of an attack. Our model relies on networks of known hostilities and past military conflicts. Therefore, this model assumes that cyber events are extensions of existing hostilities Table 6.

Table 6

Table of effects for sophisticated cyber

Cyber enemy (e_{t-1})	**Extrinsic motivation (m_t)**
+1	+1
0	0

Equation 9: Cyber-sophisticated model equation

$$y_t = AWy_{t-1} + (I - A)y_1 \quad 9$$

AQ14

3.4. Model parameters

In Sects. 3.2 and 3.3, we present five models: one naïve model for each of the three technologies, one sophisticated ~~bio~~bioweapons model and one sophisticated cyber model. Parameters that appear in these models are: A, W_H, W_F, y_1 for each of the three technologies, C and R Table 7.

Table 7

Common parameters across the models

Term	Parameter name	Description
A	Susceptibility to influence	Ratio of GDP to largest GDP
W_H	Hostility network	Military disputes from 1992 to 2007
W_F	Alliance network	Formal alliances, including NATO
y_1	Initial motivation	Estimate of initial capability and motivation
C	Nuclear hostility	Indicates whether hostile country is nuclear power
R	Nuclear reassurance	Indicates whether allied country is nuclear power

3.4.1. Susceptibility to external influence

We use countries' gross domestic product (GDP) as a measure for countries' lack of susceptibility to external influence based on previous work exploring the impact of trade in inter-state influence and conflict (Maoz et al. 2006; Gartzke 2007). Generally, countries with larger GDPs have lower expected marginal utilities to be lost from trade compared to countries with smaller GDPs. Countries with larger GDPs are better suited to absorb the negative costs associated with being perceived as developing WMD. To develop the matrix A, we use the logarithm of the ratio of a countries' GDP to the largest GDP across all countries. More precisely, $A = \mathrm{diag}(a_{11}, \ldots, a_{ii}, \ldots, a_{NN})$, where $a_{ii} = -\log(^{\mathrm{GDP}}/_{\mathrm{GDP}_{\max}})$. We use the logarithm of the ratio to slow the rate of the change as the GDP of the United States is significantly larger than most other countries.

3.4.2. Hostilities

We use the International Crisis Behavior (ICB) project at the University of Maryland and the Uppsala Conflict Data Program (UCDP) at the University of Uppsala, Sweden (Wilkenfeld et al. 2010; Daxecker 2011). The ICB project data cover violent and non-violent conflicts during the period 1918–2007. The UCDP data cover violent conflicts that caused at least 25 deaths in a calendar year during the period 1993–2010.

We only keep conflicts spanning the period from 1992 to 2007 from the ICB. This time period reflects 53 distinct hostilities and the involvement of 58 countries. ICB data only focus on the countries involved in each crisis; it does not explicitly list which coalitions were involved in each conflict. When there were more than two actors involved in a crisis, the dyad lists were coded by hand to accurately reflect coalition involvement in the crisis. Data were also filtered to ensure that only conflicts involving international actors were involved; if the crisis as recorded by the ICB project only involved one actor, then the crisis was not considered relevant to the data.

The ICB data rates conflict by the level of violence; a level "1" conflict generally means no violence, but indicates increased tensions between countries and a level "4" conflict indicates a war.

UCDP data were filtered to only keep inter-state hostilities. It reflects eight distinct hostilities, two of which had not been covered by ICB: Australia's involvement in the US invasion of Iraq, and the 2008 border dispute between Eritrea and Djibouti.

Based on the above data, we first construct a hostility network $H = [h_{ij}]$, where $h_{ij} = 1$ indicates a military conflict (ICB levels 2–4, and the two additional hostilities in UCDP data) between countries i and j, $h_{ij} = 0.5$ indicates a non-military conflict between i and j (ICB level 1), $h_{ij} = 0$ indicates no conflict between i and j. Then, we compute $W_H = AH + I - A$, where I is the identify matrix.

3.4.3. Alliances

The political alliance network is based on the formal alliance network from the Correlates of War (COW) project, using the inter-state alliance data set v3.03 (Gibler 2009). The data is first filtered to only reflect dyadic alliances in force in 2000, the most recent year available. The data set distinguishes between three kinds of treaties: a defense pact, a neutrality pact, and a non-aggression pact. For our analysis, we only include defense pacts as alliance information to reflect the level of commitment between allied countries. The alliance network drawn from COW data is expanded to reflect the military alliance among the US, Australia, New Zealand, and the UK as well as the alliance between all members of NATO.

We first construct an alliance network $F = [f_{ij}]$, where $f_{ij} = 1$ indicates a military alliance between i and j, and $f_{ij} = 0$ indicates no alliance between i and j. Then, we compute $W_F = AF + I - A$, where I is the identify matrix.

3.4.4. Initial conditions

Countries that have nuclear weapons are the United States, Russia, the United Kingdom, France, China, India, Pakistan, North Korea, and Israel. The nuclear initial condition for these nuclear powers is 1, whereas the nuclear initial condition for other countries is 0.5 following the scaling given in Fig. 1.

Unfortunately, there is considerable uncertainty about which countries have bioweapons. To alleviate this issue, we combine the list of suspected countries from multiple sources. Our sources consist of a report from the US Department of State, a report from the James Martin Center for Nonproliferation Studies, and work by Tucker (Adherence and Compliance with Arms Control 2010; Chemical and biological weapons 2008; Tucker 2000). Table 8 summarizes the countries that each source suspects of working on offensive BW. The US Department of State report is an authoritative and recent source that is important to include. Unfortunately, the US Department of State report only addresses a partial list and might have incentive to omit some proliferators for diplomatic reasons. The report by the James Martin Center for Nonproliferation Studies and the list in Tucker are

based on a compilation of available open-source data. These two sources are not limited to a subset of countries and are not subject to the same diplomatic pressure as the US Department of State report. However, these sources are error prone since they only rely on open-source data.

Table 8

List of countries suspected of maintaining BW offensive capabilities

The US ~~d~~Department of ~~s~~State	**~~James martin center for nonproliferation studies~~James Martin Center for Nonproliferation Studies**	**Tucker**
Iran, N. Korea, Russia, Syria	China, Egypt, N. Korea, Iran, Israel, Russia, Syria	Burma, China, Cuba, Egypt, India, Iran, Iraq, Israel, N. Korea, S. Korea, Laos, Libya, Pakistan, Russia, Taiwan

We construct a binary vector corresponding to each of the lists given in Table 8. In that vector, a state has value 1 if the corresponding source suspects that state. We compute a weighted sum of the three vectors by giving weight 0.4 to the list by the US Department of State, weight 0.4 to the list by the James Martin for Nonproliferation Studies, and weight 0.2 to the list by Tucker. We give a smaller weight to Tucker's list because that list is older. The fact that the US Department of State report only addresses a partial list of countries may affect the results. However, we keep that report and weigh it highly because it is an authoritative source. After computing the weighted sum, we divide that sum by 2 and add 0.5 to the division result. As a consequence, states unsuspected of working on offensive BW have an initial motivation of 0.5, and suspected states have initial motivation in the range [0.5, 1].

In the cyber area, we consider that a country has cyber weapons if the country has included a cyber security unit in its military. Lewis and Timlin (2011) identified countries that have such units by examining the policy and organizations of 133 countries. The 133 countries were selected by examining their Internet connectivity and military spending.

We consider the countries that include a cyber security united in their

military in the 1990s have initial motivation 1, as these countries have had enough time to build their capabilities. These countries are Burma, China, India, Israel, North Korea, Russia, Pakistan, South Korea, Taiwan, and the United States. We consider countries that included cyber security units in their military after year 2000 to have initial motivation 0.6. These countries are Albania, Argentina, Bahamas, Belarus, Brazil, Canada, Columbia, Cuba, Denmark, Estonia, Finland, France, Georgia, Germany, Iran, Italy, Kazakhstan, Malaysia, Netherlands, Norway, Poland, Switzerland, Turkey, Ukraine, and the United Kingdom.

Table 9 summarizes initial motivation levels for countries that have initial motivation levels for nuclear, ~~bio~~biological, and cyber weapons. All other countries have indifferent motivation levels i.e. 0.5.

Table 9

Countries with positive initial motivation levels for nuclear, ~~bio~~biological, and cyber weapons

Nuclear	**~~Bio~~Biological**	**Cyber**
Initial motivation: 1	Initial motivation: 1	Initial motivation: 1
China, France, India, Israel, North Korea, Pakistan, Russia, United Kingdom, United States	Iran, North Korea, Russia	Burma, China, India, Israel, North Korea, Russia, Pakistan, South Korea, Taiwan, United States
	Initial motivation: 0.9	
	Syria	
	Initial motivation: 0.8	
	China, Egypt, Israel	
	Initial motivation: 0.6	Initial motivation: 0.6
	Burma, Cuba, India, Iraq, Laos, Libya, Pakistan,	Albania, Argentina, Bahamas, Belarus, Brazil, Canada, Columbia, Cuba, Denmark, Estonia, Finland, France, Georgia, Germany, Iran, Italy, Kazakhstan, Malaysia, Netherlands,

	South Korea, Taiwan	Norway, Poland, Switzerland, Turkey, Ukraine, United Kingdom

4. Latent capability assessment methodology

In addition to calculating motivational levels, we conducted an assessment of latent capability associated with each of these weapons. Latent capability speaks to the potential of a country to develop these weapons provided there is national interest in doing so. We looked at a variety of different indicators that indicate national commitment to scientific and technical efforts. Broadly speaking, we assessed academic and commercial indicators, looking at research, trade, and relevant policy activities. We assign a score based on each indicator, and then combine these scores to obtain a combined latent capability score for each weapon type.

4.1. Nuclear

Due to the sensitive nature of weaponization research, we focus our analysis in the research context by counting the number of academic papers in the physics online arXiv from 1992 to 2010 that include keywords from key technologies needed to develop an indigenous nuclear capability as outlined in the Critical Technologies List (Department of Defense 1998), which highlights the technologies need at each stage of the fuel cycle, including weaponization, testing, and safeguard technologies. We choose the arXiv database for its ease in text analysis; all papers posted to the online service are in formatted LaTeX format, allowing for an easy way to differentiate between the body of the text and author affiliation. Research output is a relevant measure since there is a significant association between ownership of nuclear weapons and research output (p value < 0.001 using Fisher's exact test). We cluster research output using standard k-means analysis, with k determined by inspection of the objective function. Countries with high research output are assigned a score of '4', while countries with low research are assigned a score of '1'. For a more detailed assessment of this data and its use for remote capability assessment, particularly for nuclear data see (Kas et al. 2012) Table 10.

Table 10

Contingency table comparing arXiv research output to nuclear weapons state status

	No nuclear weapons	**Nuclear weapons**
Minimal research output (<150 papers)	164	1
Low research output (150–500 papers)	13	1
Medium research output (500–1,000 papers)	7	3
High research output (>1,000 papers)	1	3

AQ15

For commercial activity, we assessed whether the country has had a commercial nuclear energy program up through 2010 using the IAEA PRIS database International Atomic Energy Agency (2014). The database includes countries that have shut down their nuclear power activity, such as Egypt and Germany. This is included as the existence of a commercial nuclear power plant indicates significant national investment in nuclear engineering. Countries are assessed a score of '4' for having a nuclear power program and '0' for the absence of such a program. We assign a high weight to having a nuclear power program due to the known added proliferation risk of civilian nuclear power plants. While this commercial activity does not directly add to weaponization technological development, it does contribute to a nation's research and safeguard capacity.

AQ16

For policy, we assess whether the country has a military alliance with a nuclear weapons state. While the NPT explicitly forbids the sharing of nuclear engineering expertise as it relates to weapons, this speaks to the level of support given by nuclear powers to new nuclear powers, such as provision of alternative weapons or support to prevent an attack. We identify countries that have nuclear assistance based on the alliance data discussed in Sect. 3.4.3, and the list of nuclear countries discussed in Sect. 3.4.4. Countries are assessed a score of '4' for having a nuclear assister and '0' for not having a nuclear assister.

4.2. Biological

In this section, we estimate states' latent capabilities to produce BW. We take a multi-dimensional approach that examines pharmaceutical capability, dual-use biological trade and BW research. Assessing pharmaceutical capability is important since a country with a moderately sophisticated pharmaceutical industry can relatively easily produce BW Office of Technology Assessment (1993). Analyzing trade of dual-use biological equipment and commodities is relevant since these commodities and equipment can be used to produce BW. Finally, although advanced BW research may be unnecessary to produce crude BW, this research gives an insight into a country's know-how to develop advanced or novel BW.

We assign pharmaceutical capability scores based on pharmaceutical sophistication levels available in the World Medicines Situation report by the World Health Organization (Gasman et al. 2004). More sophisticated countries may encounter less difficulty developing BW and may be able to acquire more powerful BW. We assign a score of 4 to the ten states with "sophisticated industry and significant research". These ten states are responsible for the vast majority of medicine discovery. We assign a score of 3 to the 17 states with "innovative capability". These states have discovered and marketed at least one new molecular entity during the period 1961–1990. We assign a score of 2–13 states that have industries that make both ingredients and finished products. We assign a score of 1–84 states that manufacture finished products from imported ingredients. We assign score 0–42 states that have no pharmaceutical industry. Finally, we assign no score to the 23 states for which the report provides no information.

AQ17

We evaluate the strength of a country's BW research by counting the number of BW papers published by that country during the period 1980–2010. We consider a long time period to capture cases where a country performs open-domain research on a given BW agent, but performs military censorship on that research when deciding to weaponize that agent, as was the case of Russia in the 1970s and 1980s Office of technology assessment (1993). We collect all papers from Web of Science that have in their title, keywords, or abstract, the name of a weaponizable disease, e.g. anthrax or a weaponizable

agent, e.g. Bacillus anthracis. We use the list of weaponizable diseases and agents published by the Center for disease control and prevention Bioterrorism agents/diseases (2011). We exclude from the collected papers policy and economy papers as well as news articles. The existence of these papers does not indicate that a state has technical BW expertise. We are left with about 90,000 papers, mainly biological and medical and also some engineering papers. To assign research scores, we use *k*-mean clustering with $k = 4$ with the number of research papers per country as input. We assign score 4 to countries in the cluster with the largest number of papers, scores 3 to countries in the cluster with the second largest number of papers, etc.

We collect the trade of dual-use biological commodities during the period 1980–2010 from the UN Comtrade database (United Nations commodity trade statistics database 2011). The UN Comtrade database is a publicly available depository of international trade data. States inform the United Nations statistics division (UNSD) of their international trade at the end of each year and the UNSD makes the data available through the UN Comtrade database. Dual-use commodities are commodities with both civilian and military uses. Examples of these commodities are sterilization and biotechnology equipment as well as delivery equipment.

We collect the trade data by specifying the commodity codes of dual-use equipment. We obtain the list of these codes from a World Customs Organization report (World Customs Organization 2008). Unfortunately, dual-use biological commodities are typically included under large basket numbers. Due to this ambiguity, the collected trade data contain trade of dual-use commodities as well as other commodities with exclusively civilian applications. We adjust the collected trade data for inflation using the Producer Price Index (PPI) as deflator (BLS). Finally, we compute the total trade value of each country by computing the sum of the value of the country's imports and exports. To assign trade scores, we proceed similarly to research scores. That is, we use *k*-mean clustering with $k = 4$ and assign countries a score depending on which cluster they belong to. Clusters with higher trade value obtain a higher score.

4.3. Cyber

We assess cyber security latent capability through cyber security scientific research, information technology, and whether a country has cyber security institutions and policy.

Cyber security scientific research is an important indicator given that cyber security is a relatively new area. Cyber security scientific research addresses multiple problems including novel techniques to attack and defend computer systems, and cryptographic protocols. We use the number of published cyber security papers as an indicator of countries' cyber security research. We collect from SCOPUS all papers that appeared during the time period 2002–2011 in conferences that contain the word "security" in their title and that belong to the engineering or computer science areas (Scopus 2014). We obtain 28,400 papers. For each country we count the number of papers that have an author affiliated in that country. We assess information technology penetration through the number of Internet users per 100 people (Bank). Information technology penetration speaks about countries' familiarity with information technology. Similar to the ~~bio~~bioweapons latent capability scores, we assign a research score using k-mean clustering with $k = 4$ on the number of cyber security papers, and an information technology penetration score using k-mean clustering with $k = 4$ on the number of Internet users per 100 people.

We assign policy scores based on whether country has a military cyberwar policy articulated or has an identified military unit responsible of cyber security (Lewis and Timlin 2011). We assign score 4 to countries that have military cyber security policy and organizations, score 3 to countries that have civilian cyber security policy and organizations, and score 0 to countries that have no such policy and organizations. These policy and organizations are distinct from private company cyber security policy statements as these organizations respond to national interests.

4.4. Combined scores

Table 11 presents how we obtain latent capability scores for each weapon type based on research, commercial, and policy scores for each weapon type. The research, commercial, and policy scores are distinct for each type of threat due to the different impact that each context has on a country's overall

latent capability.

Table 11

Latent score calculation and source comparisons

	Nuclear	Biological	Cyber
Research (R)	arXiv papers	Web of science	SCOPUS
Commercial (C)	Nuclear power	Pharmaceutical capability	Number of Internet users per 100 people
Policy (P)	Nuclear assister	Biological dual-use trade	Cyber security institutions
Latent score	$(R+2C+P)/4$	$(R+2C+2P)/5$	$(2R+C+2P)/5$

For nuclear weapons, we give a higher weight to having civilian nuclear power. A country that has civilian nuclear power has already mastered many of the steps required to build nuclear weapons, and has some of the enriched fissile material required to develop a nuclear weapon.

For biological weapons, we put a lower emphasis on the research score, as the basic science and engineering required to use biological weapons is well understood. In contrast, the weaponization requires additional work—so additional weight is given to pharmaceutical capability and dual-use trade. Pharmaceutical capability and dual-use trade reflect both commercial and policy signals.

Finally, for cyber weapons, we give a higher weight to cyber security research and institutions. Unlike biological weapons, a significant amount of the weaponization capability is reflected in the basic science and engineering research activity, and identifying cyber security institutions reflects the military's articulated stance on developing cyber weapons.

5. Results

In this section, we present the results of our capabilities assessment. In

Sect. 5.1, we discuss the overall change in motivation values for each of the five models to demonstrate the distinct dynamics. In Sect. 5.2, we examine the overall distribution of final motivation values as well as the set of countries that have final positive motivation for each weapon type. Finally, in Sect. 5.3, we examine countries' overall risk profile by jointly taking into account countries' motivations and latent capabilities for nuclear, ~~bio~~biological, and cyber weapons.

5.1. Overall change in motivation values

Table 12 presents statistics about change in countries' motivation scores in the five models. The nuclear model and the sophisticated ~~bio~~biological and cyber models capture proliferation theory specific to nuclear, ~~bio~~bioweapons, and cyber theory, respectively. On the other hand, the naïve ~~bio~~biological (bio) and cyber models capture nuclear proliferation theory, and thus play the role of a straw man. From the table, we see that the average change in motivation is small, but that the standard deviation of that change is large for the nuclear model, the naïve bio model, the naïve cyber model, and the sophisticated cyber model. This indicates a very small change in the motivation for most countries, and a large change in the motivation of a small number of countries. The sophisticated bio model behaves differently in the sense that the average change in countries' motivation is significant.

Table 12

Summary statistics of changes in initial motivational level across different models and capabilities (194 countries total)

	Nuclear	Naïve bio	Sophisticated bio	Naïve cyber	Sophisticated cyber
Average change	−0.02	−0.01	−0.15	−0.02	0.00
Standard dev. of change	0.07	0.05	0.11	0.06	0.04
No. of countries with increased motivation	43	44	10	38	30
No. of countries with decreased motivation	86	85	183	91	29

From Table 12, we also see that the majority of countries decrease their motivations for nuclear and ~~bio~~biological weapons. This is especially the case for the sophisticated bio model, which captures nuclear reassurance. The two cyber models behave differently. When using the naïve cyber model, the number of countries that decrease their motivations is much larger than the number of countries that increase their motivations. On the other hand, with the sophisticated cyber model, we see that the number of countries that increase their motivations and the number of countries that decrease their motivations are similar. More countries decrease their motivations with the naïve cyber model because the naïve cyber model falsely assumes that an ally that has cyber capabilities provides reassurance.

Here, we see that the different motivational models show an overall decrease in motivation to develop nuclear, biological, and cyber weapons. The different models also capture different dynamics for motivation depending on the type of risk.

5.2. Motivation model results

In this section, we examine countries' motivations for each of the three weapons. These motivations represent our assessment of countries' motivations for a given weapon technology. Figure 2 presents the distribution of nuclear motivation values. From the figure we see that only a small number of countries have high final motivation for nuclear weapons. When examining the list of such countries, we find that outside of the existing nuclear powers, countries with the highest motivations for nuclear weapons include Taiwan, South Korea, and Iran.

Fig. 2

Histogram of final nuclear motivations

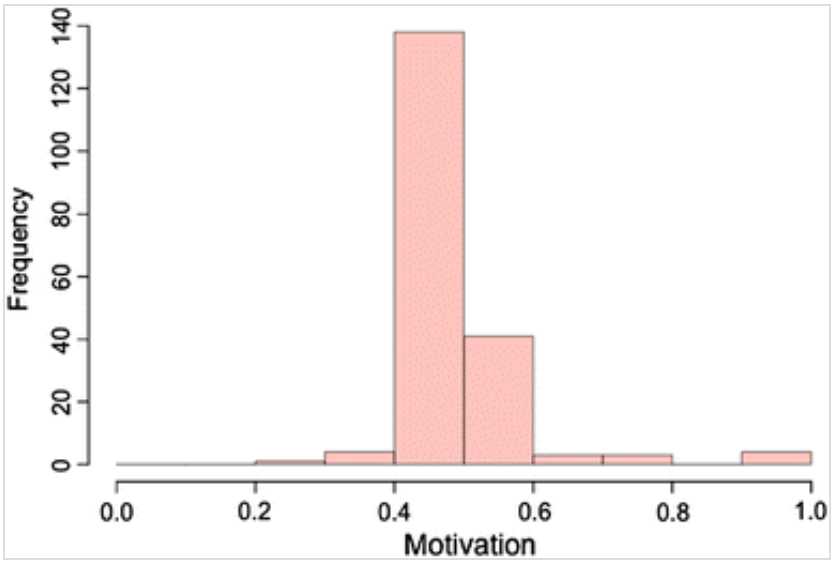


Figure 3 presents the distribution of the final motivation scores for the naïve and sophisticated bio models. From the figure, we see that the distribution of scores differs substantially across the two models. Moreover, with the sophisticated model, final scores are lower in general. However, with the sophisticated model, the number of countries with large motivations (>0.6) is slightly larger than with the naïve model. The figure shows that the sophistication and naïve models produce different results, and it is thus important to capture proliferation theory specific to the weapon technology.

Fig. 3

Histogram comparing naïve and sophisticated models of biological weapons motivation

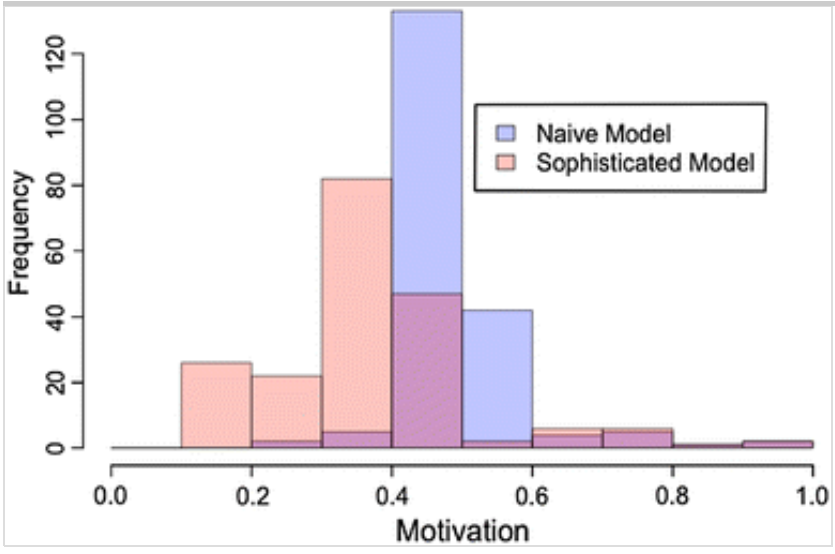


Table 13 contains the list of countries that have high motivation for BW according to the naïve and sophisticated bio models. From the table, we see significant overlap in countries interested in developing biological weapons. This is because in-kind deterrence is the main motivational factor captured in the two models.

Table 13

Countries with >0.6 motivation to develop BW

Countries in both	Countries only in sophisticated model	Countries only in naïve model
Iran, Syria, Russia, India, Israel, Pakistan, North Korea, Taiwan, Egypt	Iraq, Sudan, Georgia, Lebanon, Afghanistan, Serbia	South Korea, China, Burma
Countries are listed in descending order of motivation for each model		

According to the sophisticated model, only ten countries have an increased motivation to develop biological weapons: Sudan, Georgia, Lebanon, Afghanistan, India, Serbia, Pakistan, Taiwan, Iraq, and Syria. Comparing the naïve and sophisticated models, we see significant overlap in countries interested in developing BW. According to the sophisticated model, Iraq, Sudan, Georgia, Lebanon, Afghanistan, and Serbia also have motivation for BW. These countries have a nuclear enemy and may be interested in BW to deter that enemy. More specifically, Iraq, Sudan, and Afghanistan have hostilities with the United States, Georgia has hostilities with Russia, Lebanon has hostilities with Israel, and Serbia has hostilities with the United States, the United Kingdom, and France.

In contrast to biological weapons motivation, both the sophisticated and naïve models of cyber capabilities show high number of countries with significant motivation according to Fig. 4. From Table 14, we again see a significant overlap between countries that have positive motivation according to the sophisticated and naïve models. This is because the two models capture in-kind deterrence as an incentive for developing cyber weapons. The difference between the two models stems from the fact that the naïve model assumes that a country with cyber weapons provides reassurance to its allies, while the

sophisticated model does not make this assumption. For example, the sophisticated model finds that the United States has positive motivation for cyber weapons because the sophisticated model does not assume that Israel provides reassurance to the United States.

Fig. 4

Histogram comparing naive and sophisticated models of cyber capabilities motivation

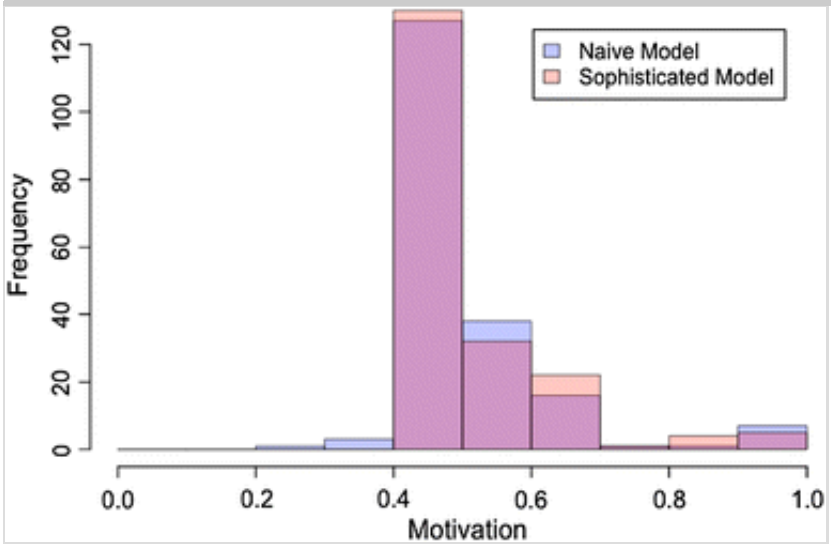


Table 14

Countries with >0.6 motivation to develop cyber weapons

Countries in both	Countries only in sophisticated model	Countries only in naïve model
Taiwan, China, South Korea, North Korea, India, Pakistan, Burma, Israel, Russia, Georgia, Thailand, Iran, Malaysia, Estonia, Cuba, Ukraine, Switzerland, Finland, Austria, Bahamas	United States, Syria, Denmark, Argentina, Kazakhstan, Belarus, Brazil, Columbia, Poland, Norway, Lebanon, United Kingdom	Albania, Germany, Canada, Italy, Indonesia
Countries are listed in descending order of motivation for each model		

For the final risk assessment, we only consider the motivations expressed under the sophisticated model as we believe these more accurately reflect the

specific motivational dynamics for each type of weapon. We have demonstrated not only that the models exhibit distinct behaviors, but that the change in behaviors also changes the countries analyzed in our risk assessment.

5.3. Overall risk profiles

In this section, we jointly examine countries' motivation and capability to develop nuclear, bio, and cyber weapons. We consider a country to be 'risky' if it is both highly motivated and highly capable of developing these weapons. We first compute the countries' risk score for each weapon as the product of countries' motivations and abilities for that weapon. Such risk values represent our assessment of countries' capabilities in each area. We then identify group of countries that have similar risk profile for these weapons. By performing a joint analysis across all three of these areas, we obtain a clearer picture of a country's overall risk profile. Traditional risk profiles, focused on individual technology types, avoid identifying joint emergent threats. Identifying and recognizing joint technological threats—such as nuclear and cyber threats—allows us to identify emergent threats and results in a different set of countries to watch than traditional approaches.

When computing a country's risk score for a given weapon, we use the motivation score from the model that we believe most appropriate for that model. That is, we use the nuclear model, the sophisticated ~~bio~~biological model, and the sophisticated cyber model. A table of top-scoring risk countries by country and technology type is included as an appendix.

We use nuclear, bio, and cyber risk scores as input to the *k*-means clustering algorithm. To find the appropriate number of clusters, we use the standard approach of inspecting the objective function of within group sum of squares and obtain $k = 4$.

Figure 5 presents the four clusters the clustering algorithm finds. To gain insight into the characteristics of these clusters, we examine Table 15, which contains statistics about the four clusters.

Fig. 5

Grouping of countries' overall risk

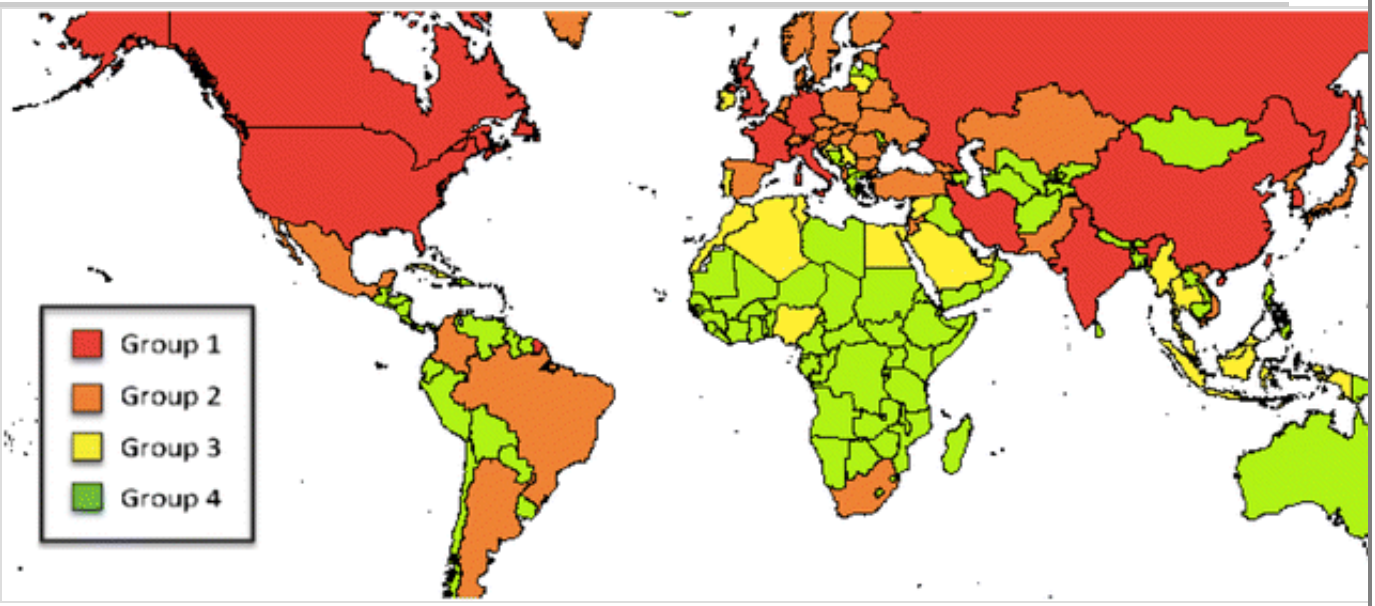


Table 15

k-means group summary statistics

Group	**1**	**2**	**3**	**4**
Size	13	35	22	124
Within group sum of squares	17.8	23.5	7.4	13.6
Nuclear risk score center	2.16	1.20	0.25	0.28
~~Bio~~Biological risk score center	1.57	0.72	1.25	0.43
Cyber risk score center	2.57	1.38	0.84	0.40

The cluster centers give a general assessment of the average group member's profile, and the within group sum of squares is an indicator of the amount of variance from the "average" group member profile. The highest risk group, group 1, can be characterized as high risk countries with established industrial bases for nuclear, biological, and cyber capabilities. This group includes almost all of the established nuclear powers, as well as Canada, Germany, Iran, Israel, Italy, South Korea, and Taiwan. The second highest risk group, group 2, includes countries that have an established nuclear capabilities base, but also have significant investments in cyber capabilities

and infrastructure. This group is considered riskier than group 3 due to a higher risk score for nuclear capabilities. It should be noted, however, that group 3 has the second highest biological risk score. Finally, we see that the majority of countries fall into group 4, which can be classified as an overall low risk profile—it has the lowest overall risk score for biological and cyber, as well as the second lowest risk score for nuclear capabilities.

The relatively high within group sum of squares for groups 1 and 2 indicate that there is a significant amount of variance in overall capabilities from the "center" risk scores for that group—in the case of group 2, potentially due to the high number of countries in that group. However, it also indicates that these countries have developed the industrial and organizational capacity to develop these types of weapons Table 16.

Table 16

Country membership in groups 1, 2, and 3

Group 1	Group 2	Group 3
Canada, China, France, Germany, India, Iran, Israel, Italy, Korea, Russia, Taiwan, United Kingdom, United States	Albania, Argentina, Armenia, Austria, Bahamas, Belarus, Belgium, Brazil, Bulgaria, Columbia, Czech Republic, Denmark, Estonia, Finland, Georgia, Hungary, Japan, Jordan, Kazakhstan, Mexico, Netherlands, North Korea, Norway, Pakistan, Poland, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, Vietnam	Algeria, Burma, Croatia, Cuba, Egypt, Indonesia, Ireland, Kuwait, Lithuania, Malaysia, Morocco, New Zealand, Nigeria, Portugal, Saudi Arabia, Serbia, Singapore, Syria, Thailand, Tunisia, United Arab Emirates

Overall, it is surprising to see that despite the high cost of investment in nuclear capabilities, countries in group 2 have invested in nuclear and cyber weapon capabilities over biological capabilities. Group 3, in contrast, has invested in biological capabilities significantly, and has not invested significantly in cyber capabilities. Most importantly, we see that ~~the most at risk countries do not invest in these capabilities independently~~the majority of countries in the table above are in groups that have invested in multiple types of capabilities:: group 1 countries have invested in all three technology types,

and group 2 countries have invested in two technology types simultaneously. This suggests that future policy work should assess these types of risk posed by these countries in conjunction—and not in isolation of the other threats that the country might pose. For example, the India–Pakistan rivalry is traditionally thought of primarily in terms of escalating nuclear threats. However, Pakistan is also developing its cyber capabilities—and WMD policy addressing the rivalry should also address cyber capabilities.

AQ18

6. Future work

Our work presented here is far reaching: it incorporates a significant amount of information, and provides useful outputs to aid policymaker decisions. By jointly assessing state-level risk scores, we have established a baseline for assessing these WMD risks at a global scale. There are, however, several further areas for development, including performing joint motivation assessments, improved remote detection by incorporating social media inputs, and understanding the dynamics of cyber threats.

The motivation assessment models assume that countries' decisions to pursue various weapons are independent. In reality, a country interested in strengthening its military capabilities examines multiple options simultaneously. For example, Horowitz and Narang (2014) find that countries that pursue nuclear weapons are also likely to pursue biological and chemical weapons, but that countries become less interested in biological and chemical weapons once they acquire nuclear weapons. There is also some evidence showing that substate actors and terrorist groups will pursue WMD if receiving implicit support from a state government (Asal et al. 2012). One interesting future work direction is to design a motivation assessment model that simultaneously captures multiple capabilities, and considers the risk posed by state-supported terror groups.

AQ19

Another approach to extend the motivational methodology is to include sentiment analysis based on political leadership rhetoric and social media analysis. Rhetoric and sentiment assessment from social media reflect national and cultural norms, which in turn drive a major theory of nuclear

proliferation: constructivism. By incorporating cultural norms and attitudes into the motivational model, we would have a better understanding of the constructivist dynamics driving the motivation of countries to develop WMD.

Finally, the dynamics of cyber threats are not well understood. Unlike traditional WMD threats, which are rare in occurrence, cyber events take place at a large scale on a daily basis. Many of the events are limited to private business, but private sector intrusions can be linked directly to national interests in major industries such as defense contracting, finance, and critical infrastructure protection. Our cyber motivation model captures state-driven motivation to develop better offensive capabilities. However, it does not capture state-level motivation to coordinate and collaborate to develop more effective cyber security, and it does not address the difficulty of attribution in responding to state-driven events.

7. Conclusion

In this paper, we systematically assess all countries' nuclear, bio, and cyber capabilities using an approach that examines both countries' motivations and latent capabilities. We first separately assess countries' nuclear, bio, and cyber capabilities. Then, we examine countries' overall risk when taking into account countries' capabilities in the three areas. Simultaneously taking into account the three areas provides a better perspective than when separately examining each of these areas.

To assess countries' motivations for a given weapon type, we adapt Friedkin socio-cultural model to capture experts' opinions about why countries seek this weapon type. When adapting the Friedkin model to assess motivations for ~~bio~~biological and cyber weapons, we find that it is important to capture the specificities of the proliferation of these weapons rather than naively assuming that the proliferation of these weapons is similar to nuclear proliferation. To assess countries' latent capabilities in each area, we look for relevant signals from a country's research, commercial, and policy activities.

When simultaneously examining countries' risk for the three weapon types, we find four risk profiles. The highest risk group has strong bases in the three areas, and consists of most nuclear powers as well as Canada, Germany, Iran,

Israel, Italy, South Korea, and Taiwan. The second highest risk group poses nuclear and cyber risk, but little ~~bio~~bioweapons risk. The third riskiest group poses some ~~bio~~bioweapons risk, but little nuclear and cyber risk. Finally, the vast majority of countries pose very little risk for the three weapon types.

This work represents a significant step in integrating computational approaches with real-world data in this field. It allows policymakers to directly see how small changes in assumptions, such as perceived motivations as a result of in-kind deterrence and latent capability, can directly change outcomes of the model. It allows individuals with access to new and additional data to fine-tune model results.

Acknowledgments

This work is supported in part by the Defense Threat Reduction Agency (DTRA) under Grant HDTRA11010102 and the center for Computational Analysis of Social and Organizational Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of DTRA or the US Government.

8. Appendix A: Individual risk score assessments

This appendix includes a global map of the risk scores and a table indicating the top 20 countries with the highest risk scores for each individual technology. Risk scores should not be directly compared across technologies due to the different types of risk they represent and due to the different methodologies used to create the latent scores Figs. 6, 7, 8; Tables 17, 18, 19.

Fig. 6

Map of nuclear risk scores; *darker red* indicates higher score

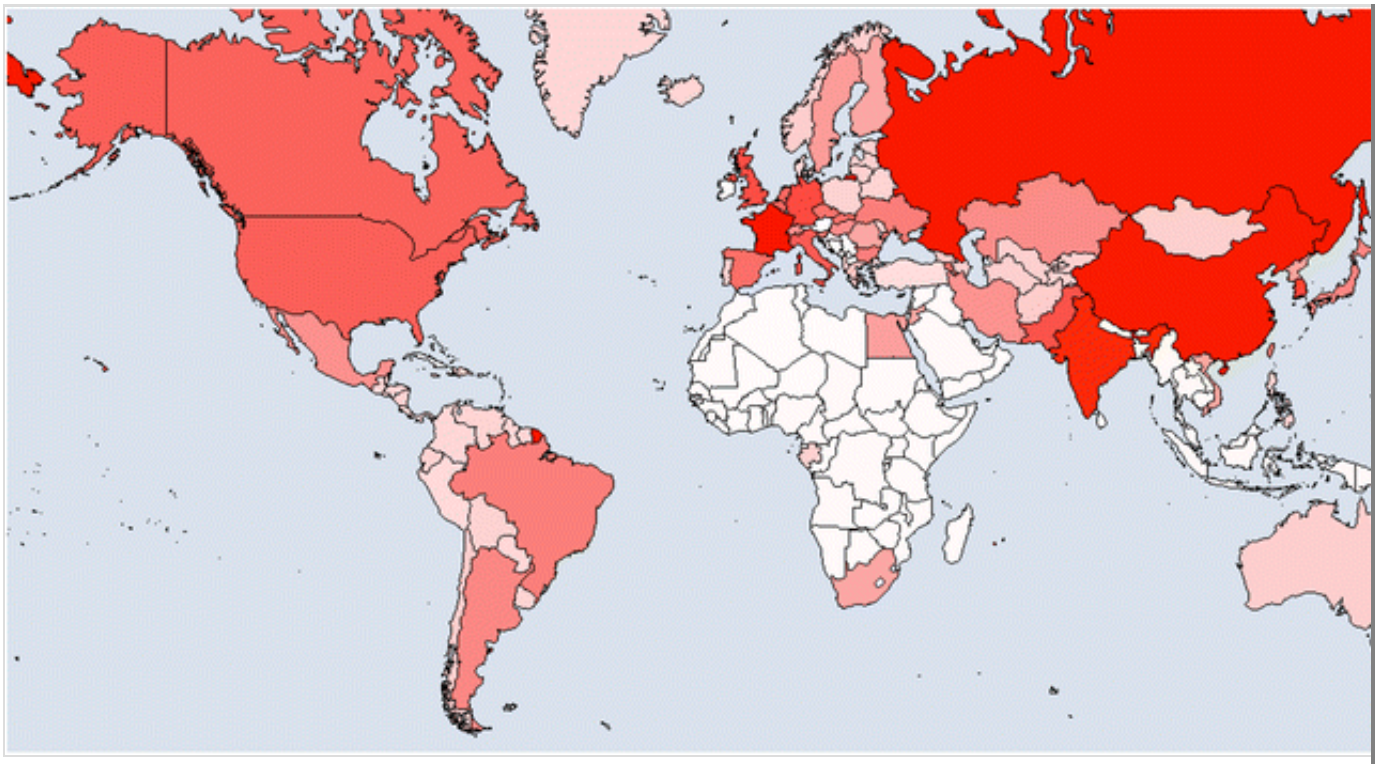


Fig. 7

Map of biological risk scores; *darker green* indicates higher risk

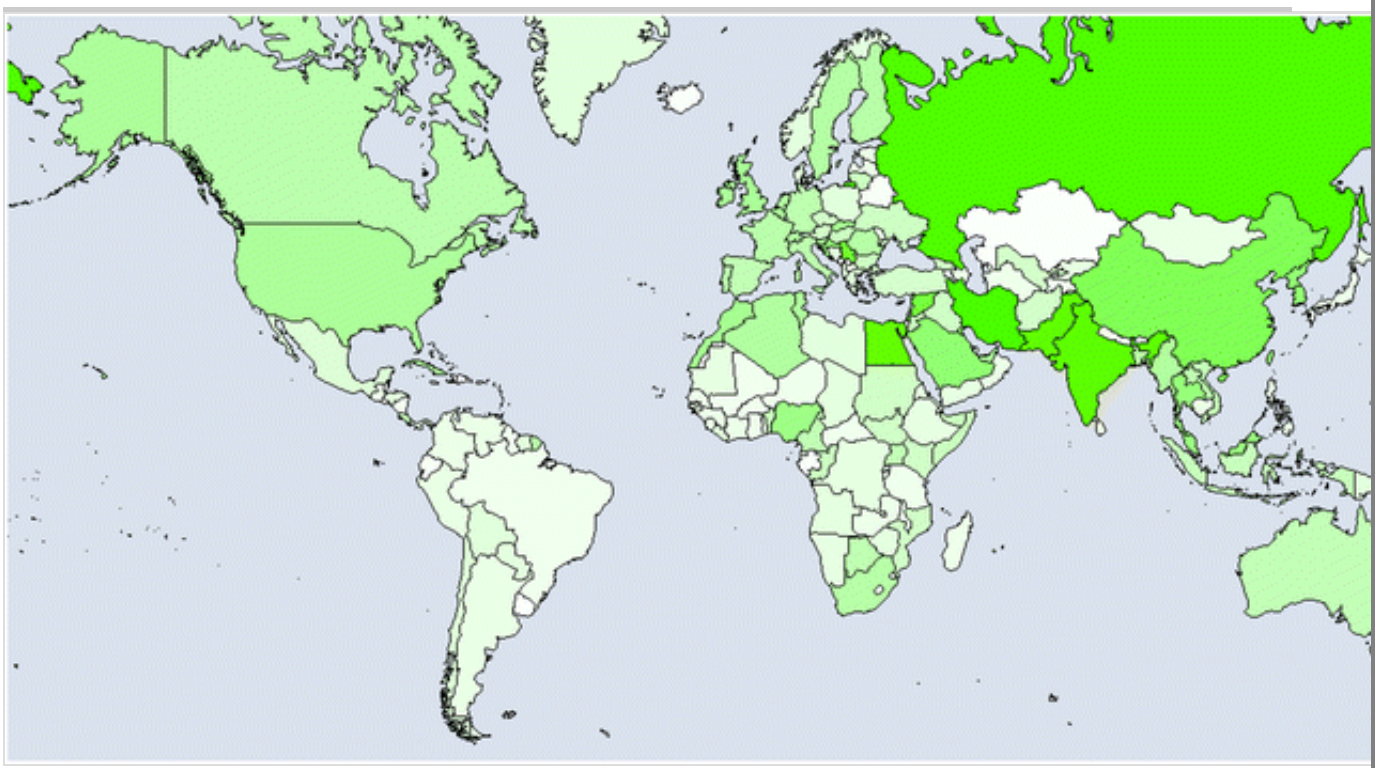


Fig. 8

Map of cyber risk scores; *darker blue* indicates higher risk

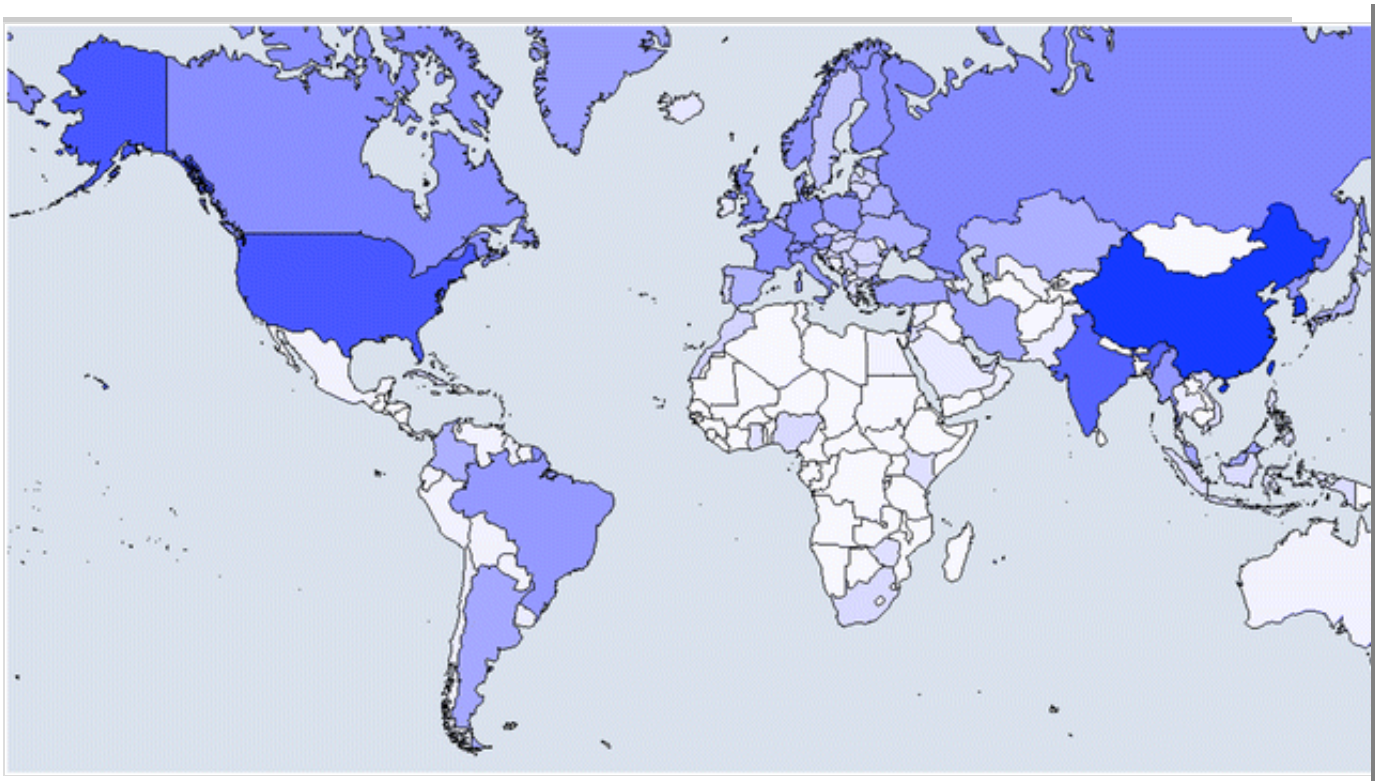


Table 17

Table of top 20 highest risk scoring countries for nuclear assessment

Score	Country	Score	Country
3.1	France	2.0	Canada
3.0	Russia	1.9	Netherlands
3.0	China	1.9	Belgium
2.7	India	1.8	Spain
2.4	South Korea	1.8	Slovakia
2.3	Germany	1.7	Czech Republic
2.2	United Kingdom	1.7	Armenia
2.2	Pakistan	1.6	Ukraine
2.0	Italy	1.6	Slovenia
2.0	United States	1.6	Bulgaria

Table 18

Table of top 20 highest risk scoring countries for biological assessment

Score	Country	Score	Country
2.9	Iran	1.5	Saudi Arabia
2.6	Russia	1.5	North Korea
2.3	India	1.5	South Korea
2.2	Israel	1.4	Taiwan
2.2	Pakistan	1.4	Thailand
2.1	Egypt	1.4	Croatia
1.9	Serbia	1.4	Malaysia
1.9	Syria	1.3	Nigeria
1.7	China	1.2	Morocco
1.5	Kuwait	1.2	Slovakia

Table 19

Table of top 20 highest risk scoring countries for cyber assessment

Score	Country	Score	Country
3.6	Taiwan	2.1	Germany
3.6	China	2.1	Canada
3.5	South Korea	2.1	Switzerland
3.0	United States	2.0	Finland
2.8	India	2.0	Austria
2.7	Israel	2.0	Norway
2.2	United Kingdom	1.9	Burma
2.2	Bahamas	1.9	Italy
2.2	Russia	1.9	North Korea
2.1	France	1.9	Poland

AQ20

References

Abraham I (2006) The ambivalence of nuclear histories. Osiris 21(1):49–65. doi:10.1086/507135

Adler E (1992) The emergence of cooperation: national epistemic communities and the international evolution of the idea of nuclear arms control. Int Org 46(1):101–145

Adherence and Compliance with Arms Control (2010) Nonproliferation, disarmament agreements and commitments

Asal VH, Ackerman GA, Rethemeyer RK (2012) Connections can be toxic: terrorist organizational factors and the pursuit of CBRN weapons. Stud Confl Terror 35(3):229–254. doi:10.1080/1057610X.2012.648156

~~Bank World~~World Bank Indicators http://data.worldbank.org/indicator

Betts RK (1993) Paranoids, pygmies, pariahs and nonproliferation revisited. In: Davis ZS, Frankel B (eds) The proliferation puzzle: why nuclear weapons spread (and what results). Frank Cass, Portland

Bioterrorism agents/diseases. Center for disease control and prevention (2011) Accessed September. http://www.bt.cdc.gov/agent/agentlist-category.asp

BLS Producer price index. Bureau of labor statistics. http://www.bls.gov/ppi

Carley KM (2011) Dynamic network analysis and modeling for CANS. In: Bragg B, Popp G (eds) A guide to analytic techniques for nuclear strategy analysis. NSI, Oklahoma, pp 191–202

Chemical and biological weapons (2008) James Martin Center for nonproliferation studies. http://cns.miis.edu/cbw/possess.htm

Dai X (2007) International institutions and national policies. Cambridge University Press, New York

Davis ZS (1993) The realist nuclear regime. In: Davis ZS, Frankel B (eds) The proliferation puzzle: why nuclear weapons spread (and what results). Routledge, New York

Daxecker UE (2011) Rivalry, instability, and the probability of international conflict. Confl Manag Peace Sci 28(5):543–565. doi:10.1177/0738894211418591

De Mesquita BB, Stokman FN (1994) European community decision making: models, applications, and comparisons. Yale Univ Pr, New Haven

Department of Defense (1998) Military Critical Technologies List. Department of Defense

Elliott D (2011) Deterring strategic cyberattack. IEEE Secur Priv Mag 9(5):36–40

Frankel B (1991) Opaque Nuclear Proliferation. Psychology Press

Friedkin Noah E (1998) A structural theory of social influence. Cambridge University Press, New York

Fuhrmann M (2009) Taking a walk on the supply side the determinants of civilian nuclear cooperation. J Confl Resolut 53:181–208

Gartzke E (2007) The capitalist peace. Am J Polit Sci 51(1):166–191

Gasman N, Mariko M, Creese A (2004) The world medicines situation. World Health Org

Gibler DM (2009) International military alliances. CQ Press, Washington, DC, pp 1648–2008

Harney R, Brown G, Carlyle M (2006) Anatomy of a project to produce a

first nuclear weapon. Sci Glob Secur 14:163–182

Horowitz MC, Narang N (2014) Poor Man's atomic bomb? exploring the relationship between "weapons of mass destruction". J Confl Resolut 58(3):509–535. doi:10.1177/0022002713509049

Huth PK (1999) Deterrence and international conflict: empirical findings and theoretical debates. Annu Rev Polit Sci 2(1):25–48

Hymans JEC (2010) When does a state become a 'nuclear weapon state'? an exercise in measurement validation. Nonprolif Rev

International Atomic Energy Agency (2014) Power reactor information system. http://www.iaea.org/pris/

Jacques EC (2006) Hymans, The psychology of nuclear proliferation: identity, emotions and foreign policy. Cambridge University Press, Cambridge

Jervis Robert (1979) Deterrence theory revisited. World Polit 31(2):1–37

Jervis R (2003) The confrontation between Iraq and the US: implications for the theory and practice of deterrence. Eur J Int Relat 9(2):315–337. doi:10.1177/1354066103009002006

Jo DJ, Gartzke E (2007) Determinants of nuclear weapons proliferation. J Confl Resolut 51(1):167–194

Kaplan FM (1983) The wizards of armageddon. Stanford University Press, Stanford, CA

Kas M, Khadka AG, Frankenstein W, Abdulla AY, Kunkel F, Carley LR, Carley KM (2012) Analyzing scientific networks for nuclear capabilities assessment. J Am Soc Inf Sci Technol 63(7):1294–1312. doi:10.1002/asi.22678

Kroenig M (2010) Exporting the Bomb: Technology Transfer and the

Spread of Nuclear Weapons. Cornell Univ Pr, Ithaca

Lebovic JH (2007) Deterring international terrorism and rogue states. Routledge, New York

Lewis JA, Timlin K (2011) Cybersecurity and cyberwarfare. Center for strategic and international studies

Libicki MC (2009) Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, CA

Litwak RS (2007) Regime change: US strategy through the prism of 9/11. Woodrow Wilson Center Press, Washington

Maoz Z, Kuperman RD, Terris L, Talmud I (2006) Structural equivalence and international conflict. J Confl Resolut

Meyer S (1984) The dynamics of nuclear proliferation. University of Chicago Press, Chicago

Mezzour G, Frankenstein W, Carley KM, Carley LR (2014) Systematic assessment of Nation-States motivations and capabilities to produce biological weapons. Carnegie Mellon University, Pittsburgh

Montgomery AH, Sagan SD (2011) The perils of predicting proliferation. In: Rauchhaus R, Kroenig M, Gartzke E (eds) Causes and consequences of nuclear proliferation. Routledge, New York, pp 294–329

Morgan PM (2003) Deterrence now. Cambridge University Press, Cambridge

Nolan J, Strauss M (1997) The rogues' gallery, stealing the fire. Brown J World Aff 4(1):21–38

Office of Technology Assessment (1993) Technologies underlying weapons of mass destruction

Rublee MR (2009) Nonproliferation norms. University of Georgia Press, Athens

Sagan SD (1996) Why do states build nuclear weapons?: three models in search of a bomb. Int Secur 21(3):54–86

Sagan SD (2000) The commitment trap: why the United States should not use nuclear threats to deter biological and chemical weapons attacks. Int Secur 24(4):85–115 (The MIT Press)

Sagan SD (2010) Nuclear latency and nuclear proliferation. In: Potter WC, Mukhatzhanova G (eds) Forecasting nuclear proliferation in the 21st century, 1st edn. Stanford University Press, Stanford, pp 58–79

Scopus (2014) Accessed February 21. http://www.elsevier.com/online-tools/scopus

Smith DD (2006) Deterring America. Cambridge University Press, Cambridge

Solingen E (2007) Nuclear logics: contrasting paths in East Asia and the Middle East. Princeton University Press, Princeton

Stoll JR (1996) World production of latent nuclear capacity. http://es.rice.edu:80/projects/Poli378/Nuclear/Proliferation/proliferation.html

Talbert MD, Zentner GL, Coles RJ (2005) Nuclear proliferation technology trends analysis PNNL-14480, vol 1. Office of Scientific and Technical Information, DOE, Oak Ridge

Tannenwald N (1999) The nuclear taboo: the United States and the normative basis of nuclear non-use. Int Org 53(3):433–468 (The MIT Press)

Thayer BA (1995) The causes of nuclear proliferation and the utility of the nuclear non-proliferation regime. Secur Stud

Trachtenberg M (1991) History and strategy. Princeton University Press, Princeton

Tucker J (2000) Motivations for and against proliferation: the case of the middle east. In: Zilinkas R (ed) Biological warfare: modern offense and defense. Lynne Rienner Publishers, Boulder

United Nations commodity trade statistics database (2011) UN. Accessed August. http://comtrade.un.org/db/

Waltz KN (2010) Theory of international politics. Waveland Press, Long Grove, IL

Waltz K, Sagan SD (2002) The spread of nuclear weapons, 2nd edn. WW Norton & Company, New York

Wilkenfeld J, Brecher M, Hewitt J, Beardsley K, Eralp P (2010) International crisis behavior dataset. http://www.cidcm.umd.edu/icb/data/

Wohlstetter AJ (1979) Swords from plowshares. University Of Chicago Press, Chicago

World Customs Organization (2008) Classification of the biological dual-use items of the convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxin weapons and their destruction. Brussels