A System Dynamics Model of Cyber-conflict

Dana Polatin-Reuben
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
dana.polatin-reuben.2011@bristol.ac.uk

Richard Craig
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
richard.craig@bristol.ac.uk

Theodoros Spyridopoulos
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
th.spyridopoulos@bristol.ac.uk

Theo Tryfonas
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
t.tryfonas@bristol.ac.uk

***Abstract*—In this paper we try to determine whether a potential state-aggressor in a recent cyber attack can be identified through an understanding of shared international dependencies between nations. Combining the International Affairs and Systems Science disciplines, we put forth a system dynamics model of cyber conflict which may facilitate the identification of a culpable state or states in a cyber attack through publicly available information. Having identified 22 countries with military or civilian cyber capability, data on economic trade imports and diplomatic relationships were combined to identify dependencies, or countries upon which dependent countries relied for trade or military collaboration. The system dynamics model simulates diplomatic tension between two countries to estimate the probability of a cyber conflict. Nine case studies, in which the likely cyber combatant was identified, are used to test the model. Initial results yielded a number of prior indicators of cyber conflict, such as dips in trade imports from future cyber combatants up to 2 years before a launched cyber attack.**

***Index Terms*—Cyber Conflict, System Dynamics, International Relations, Interdependencies**

I. Introduction

Cyber warfare is an evolving phenomenon of concern to both computer scientists and the international diplomatic community. As Internet and information technologies mature, combatant states are taking to the nebulous regions of cyberspace to conduct strategic operations against enemy targets. These can manifest as espionage, information control, or even the sabotage of real-world targets [1].

Given the strategic importance of cyber warfare and the increasing frequency of cyber attacks, it is unsurprising that international militaries have invested heavily in research on this topic. This is often undertaken in collaboration with interested academics from the International Affairs and, increasingly, Computer Science disciplines. While approaching the topic from a Computer Science perspective is relatively new, the International Affairs community has been producing comprehensive texts detailing social science theories of information and cyber warfare for over a decade [2][3][4].

Many questions about cyber warfare remain. Determining the culpable party or parties in a cyber attack is difficult given that states often use third parties who cannot be easily traced and are not held accountable to the same international laws and treaties as governments [1]. Often the only clue that a cyber attack has a state sponsor is the complexity of the virus itself; the Flame virus developed a new variation of the chosen-prefix collision attack, indicating the experience of the creators [5].

Research in the area generally takes two forms. The first is research from within the International Affairs discipline, often in collaboration with an interested military, which presents social science theories on information and cyber warfare [2][3][4][6][7]. While these theories are comprehensive and well-researched, they fall firmly within the realm of social science and cannot be independently tested and verified in the same way as a scientific theory. The second form of research comes from the Computer Science discipline, which focuses on the related topic of corporate espionage and particularly insider and outsider threats [8][9]. However, comprehensive models of the complexities of information and cyber warfare have not previously been attempted, in part because computer scientists are more interested in simulating the attack patterns of computer viruses than the socio-political phenomena which lead to cyber conflict.

This paper combines the two disciplines of International Affairs and Systems Science by creating a system dynamics model of information and cyber warfare which draws on both theories put forth from the International Affairs community and system dynamics models of cyber security issues previously created by computer science professionals. The model illustrates the relationship between the diplomatic interactions of two countries, their trade imports, regional interests, potential capability and the probability that they will engage in conflict.

II. Exploring International Dependencies

The United Nations Institute for Disarmament Research conducted a preliminary assessment of national doctrine and organisation of state cyber-capability in 2011, which was used to select the 22 countries to include for general data collection [7]. The majority of these states have military doctrine and organisations in place for waging cyber warfare or dealing with cyber security issues, although a minority of states slated for inclusion have only instituted civil policies and organisations for cyber security issues.

States with active military policy covering information and cyber warfare include Argentina, Australia, Brazil, China, Estonia, France, Georgia, Germany, India, Iran, Israel, the Netherlands, North Korea, Russia, South Korea, the United Kingdom and the United States. States with civil organisations combating information and cyber warfare include Japan, New Zealand, Nigeria and Pakistan. Data was additionally gathered for Iraq because, although it has since undergone regime

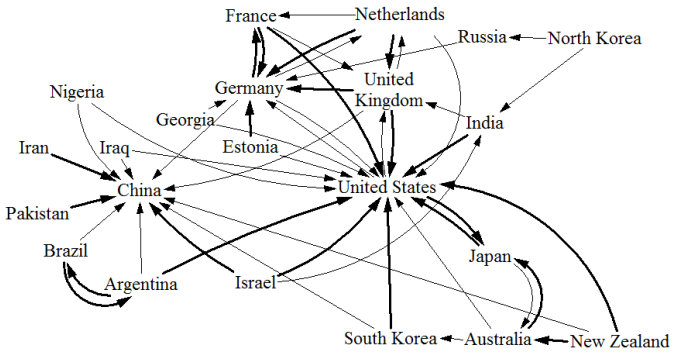

Figure 1. Analysis of primary (bold) and secondary (thin) dependencies of examined countries.

change, it features in an important case study in information and cyber warfare and has been discussed by multiple authors. The above countries were selected based on how strong their cyber capability is, how computerised their infrastructures are and whether they featured in any previous case studies on information and cyber warfare.

Open-source data was gathered for each of the 22 countries in the dataset. Most critical was data on trade imports, which was used as an indicator for numerous other variables such as regional interests and international dependencies. Diplomatic indicators were also examined, and a scale was created to quantify the 462 diplomatic relationships in the dataset.

The dependencies variable was created to attempt to quantify diplomatic alliances in the thought that two countries with shared alliances would be less likely to engage in cyber conflict. An analysis of primary and secondary dependencies of countries within the dataset is shown in Figure 1. Two types of dependencies are defined below:

- A primary dependency is a country within the dataset which is in the top three for both selling imports to and buying exports from the dependent country, and whose diplomatic relationship with that country involves military collaboration.
- A secondary dependency is a country which is either in the top three for imports or exports with the dependent country with a military relationship, or is in the top three for both imports and exports with the dependent country with a neutral or positive diplomatic relationship.

The United States serves as a dependency for 15 countries in the dataset – over half of the 22 countries represented. Of these 15 countries, eight count the United States as a primary dependency. China is the second most depended upon nation with 11 countries, or half the dataset, counting it as a dependency. However, only three countries count China as a primary dependency, which indicates that while China's economy is rising it is less likely to form military alliances.

China is the only country in the dataset to have no dependencies. This means that China does not depend on any other country in the dataset either militarily or economically, making China the 'freest' actor in the dataset – China does not have to worry about the reactions of allied countries to a cyber attack.

Germany is not far behind China in the number of dependent countries. Seven countries in the dataset count Germany as a dependency, with four considering Germany to be a primary dependency. Six of the 7 countries which count Germany as a primary or secondary dependency are in or near Europe, indicating that Germany serves as a regional hub for alliances. With the inclusion of more countries in the dataset, other countries such as Japan could also emerge as regional hubs.

Strained relationships and dependencies have not been depicted, revealing surprising dependencies. For example, as North Korea's relationship with China is currently strained, North Korea's secondary dependencies on India and Russia can be examined with more scrutiny. Likewise, as Pakistan's relationship with the United States has deteriorated over what Pakistan views as threats to its sovereignty, Pakistan has formed a primary relationship with China which may grow closer in future. China and the United States have a mutual strained primary dependency – this could be a factor in cyber hostilities and in itself merits further research.

III. ANALYSIS OF CYBER CONFLICT CASES

The case studies presented below were used to build the system dynamics model. Each case study was analysed on several variables, including shared primary and secondary dependencies between cyber combatants, shared regional interests, trade imports and their diplomatic relationship at the time of the cyber attack.

1) North Korea: In the midst of international diplomatic tension surrounding North Korea's nuclear capability, a cyber attack on 20th March 2013 struck approximately 48,000 computers and servers in South Korea [11]. Critical banking and broadcasting infrastructure was disrupted during the attack. Suspicions that North Korea masterminded the attack were confirmed when investigators in Seoul linked some of the code to known North Korean malware.

2) Stuxnet virus: Farwell and Rohozinski [1] give a very detailed summary of the Stuxnet virus as well as put it into the context of emerging trends in cyber warfare. Described by Computer World as 'one of the most sophisticated and unusual pieces of software ever created', it is now known that the Stuxnet virus was a cyber attack launched by joint aggressors Israel and the United States against nuclear facilities in Iran in order to delay progress on its nuclear programme [12].

3) Flame virus: Discovered in May 2012, the Flame virus was first analysed by CrySyS Lab in Hungary [13]. Designed for broad intelligence-gathering, it is the most advanced malware ever found whose creators developed a new variation of the chosen-prefix collision attack and subsequent to its discovery sent a 'suicide' command removing the malware from some infected computers [5][14]. As the vast majority of Flame targets were in Iran, the cyber combatants are assumed to be the same as in Stuxnet – United States and Israel as co-aggressors, with Iranian infrastructure the intended target.

4) GhostNet virus: In March 2009, researchers at the Information Warfare Monitor reported a large-scale cyber spying operation against a number of Tibetan institutions

[15]. GhostNet compromised multiple critical infrastructures which included 'computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs.' GhostNet gained unprecedented access to sensitive information concerning the expatriate Tibetan community, indicating that the Chinese government was involved at some stage of the development or deployment of the virus. GhostNet is unique among the case studies in that it affected multiple victims in the dataset.

5) China and the United States: In addition to the GhostNet attacks discussed above, China also frequently deploys cyber attacks against the United States in order to gain information about American cyber capability. In a 2012 report commissioned by the United States Congress about Chinese cyber capability, Northrop Grumman warned that 'Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict'[16]. One example of a potential Chinese attack on American infrastructure is that of the penetration of and subsequent data theft from RSA, a world-leading provider of network encryption devices, in early 2011. Lockheed Martin, an American defence firm, subsequently disclosed a successful large-scale penetration of their network carried out with information gleaned from the attack on RSA.

6) Russia and Estonia: Miller and Kuehl [17] provide an overview of two case studies: those of Estonia and Georgia, which both had cyber confrontations with Russia. Estonia, whose critical infrastructure is heavily computerized, became the target of one of the first instances of coordinated cyber warfare in 2007 after relocating the Bronze Soldier of Tallinn, a Soviet-era statue. The attacks targeted both public and private sector websites and infrastructure, including the websites of the Estonian parliament and the president. Evidence points to the purchase of a botnet from 4-8th May 2007 for the explicit purpose of launching these attacks.

7) Russia and Georgia: The cyber war between Russia and Georgia during the summer of 2008 was launched in conjunction with Russian military action [17]. Russia's cyber attacks were mostly conducted in order to prevent Georgia from presenting its point of view on Russia's military hostilities to the outside world. 'The evolution of Russian strategic thinking throughout the 1980s and 1990s,' explains Miller and Kuehl, 'incorporated the potential to degrade national economic systems and communications networks as a means of breaking the enemy's will to resist and inflicting military and political defeat, at low cost and without the need to occupy territory.' Cyber warfare was therefore an ideal option leading up to the conflict with Georgia as it decreased the cost of combat operations.

8) Argentina and the United Kingdom: In February 2010 Argentine hackers defaced the website of the Falkland Islands' weekly newspaper, Penguin News, with material supporting Argentina's claim of sovereignty over the Falklands [18]. This attack was launched amidst diplomatic tensions between Argentina and the United Kingdom over proposed oil drilling in Falklands waters. While this cyber attack was small and not necessarily funded by the Argentinian government, it was clearly motivated by the sovereignty issues surrounding the Falkland Islands.

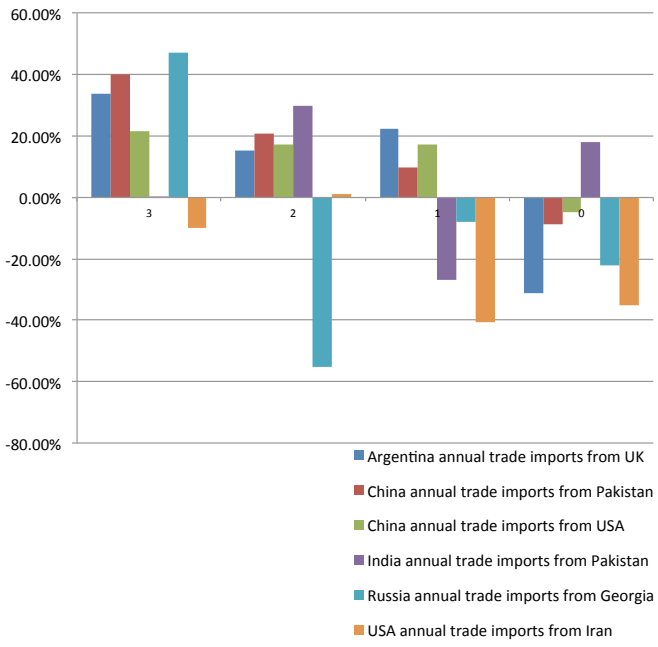

Figure 2. Annual trade imports from victim countries expressed as a percentage of the previous year's imports.

9) India and Pakistan: India and Pakistan have been engaged in cyber conflict since May 1998, soon after India announced its first nuclear test [19]. The most recent round of cyber attacks began in late 2010, with Pakistani hackers calling themselves the 'Pakistani Cyber Army' compromising the website of India's top police agency in addition to mass defacement of Indian websites 'in response to the Pakistani websites hacked by "Indian Cyber Army"' [20].

A. Case Analysis and Results

The case studies were used to perform a statistical analysis on the dataset to determine open-source markers preceding cyber conflict. This was particularly successful, with the indicators identified listed below.

In 4 of 9 cases:

- Cyber combatants were in the same region.

In 5 of 9 cases:

- Victims had higher percentages of imports and exports with the aggressor compared to total trade volume than vice versa, suggesting that the victims were more dependent on trade with the aggressor.

In 6 of 9 cases:

- Two-thirds of case studies had repeat assailants, suggesting that countries which have previously waged cyber conflict are more likely than other countries to launch another attack.

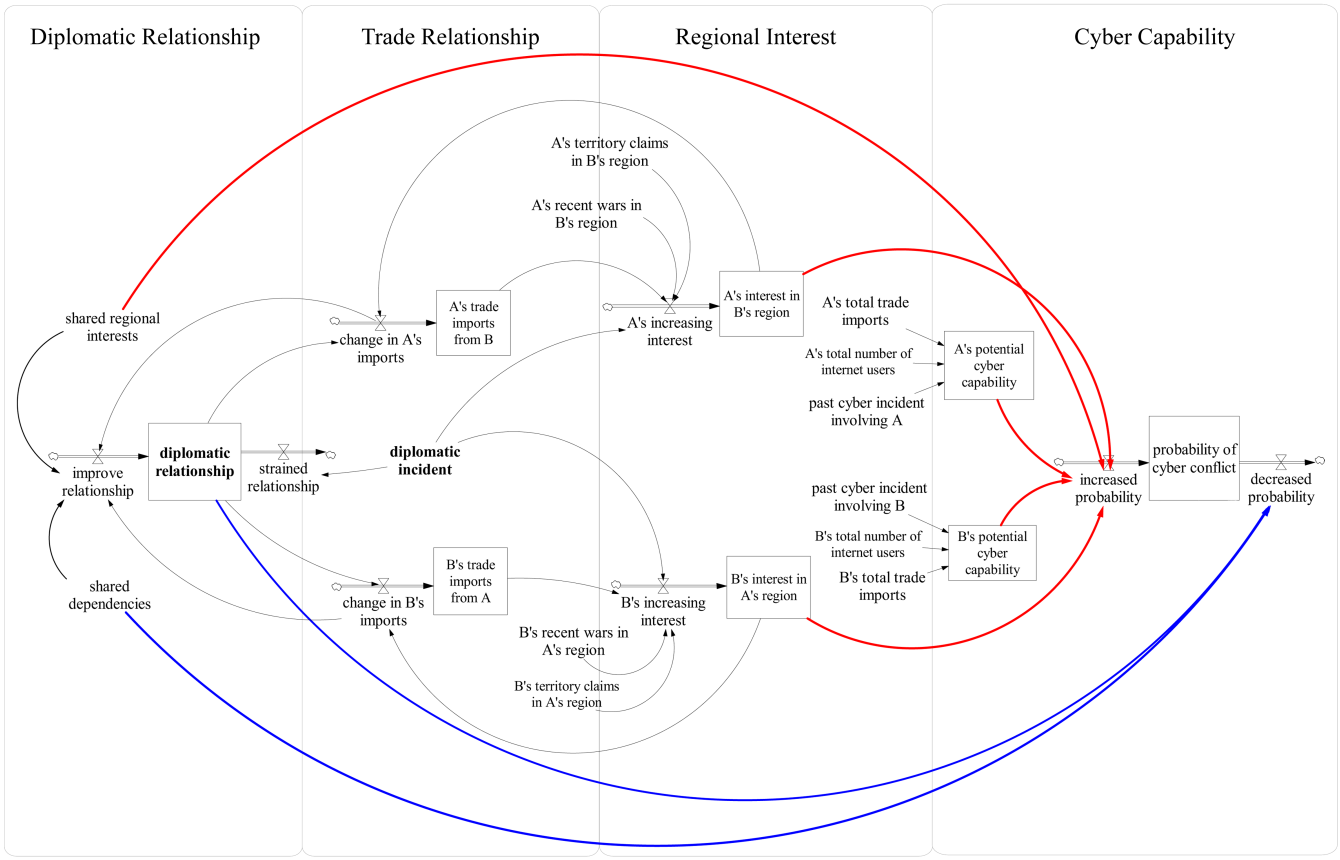

Figure 3. System dynamics model of international cyber conflict, shown with balancing loop.

- Cyber combatants shared no primary dependency, indicating that alliances are important in preventing cyber conflict.

In 7 of 9 cases:

- The attacking country had more total internet users than the victim country, indicating that the number of internet users is more important in determining potential cyber capability than is internet proliferation.
- Trade dips from victim countries were noted commonly in the year before the cyber attack.
- Trade dips from aggressor countries usually occurred the year of the cyber attack.
- Cyber combatants had territory claims in the same region.

In 8 of 9 cases:

- In all single-victim case studies, cyber combatants had a strained diplomatic relationship either as a result of a recent diplomatic incident or ongoing military conflict.
- Cyber combatants shared significant regional interests, meaning they either had each other's region within their top three for imports, or the combatant's region and at least one other shared region, or shared at least two regions.
- The victim or the aggressor had waged war in the combatant's region since 1980. In 7 of 9 cases the aggressor had waged war; the victim was belligerent in 6 of 9 cases.

The trade imports made by cyber aggressors from their victim countries in 6 of 9 case studies have been graphed above, with the imports being expressed as a percentage of the previous year's imports.

In 5 of 9 case studies trade dips occurred in 2009, following the 2008 financial crisis. This raises the question of how greater economic trends, such as the global recession seen after the 2008 financial crisis, affect a state's decision to engage in cyber conflict. It is possible that states competing for resources in the wake of an economic crisis would be more likely to launch cyber attacks to satisfy regional objectives. Additionally, cyber conflict represents an alternative to military action which is less financially and diplomatically costly.

As cyber conflict is a relatively new phenomenon, this avenue of research may be more promising in the future when more case studies have occurred and can be compared to overarching economic trends.

IV. A SYSTEM DYNAMICS MODEL

System dynamics, a discipline pioneered by Jay W. Forrester at the Massachusetts Institute of Technology starting in the 1950s, seeks to understand a given system or systems through 'the interaction between the flows of information, materials, money, manpower, and capital equipment' [10]. This approach was used to create a visual model of the escalation of diplomatic tension into cyber conflict between two countries.

System dynamics is a particularly suitable discipline for modelling information and cyber warfare as it can be used to model complex political, social and business issues. While cyber security issues have previously been modelled using system dynamics, there are few other models which dealt specifically with cyber warfare between two or more combatant states.

Our proposed system dynamics model of international cyber conflict is comprised of four different relationship domains which interact with each other to calculate the probability of cyber conflict between two nations. These are the diplomatic relationship domain, the trade relationship domain, the regional interest domain and the cyber capability domain. For each of these domains we have set a stock, as shown in Figure 3, that is either increased or decreased depending on the incoming and outgoing flow rates. Based on our analysis of 9 case studies as presented in the next section, we concluded that shared regional interest, shared dependencies, diplomatic incidents, territory claims and recent wars are the main variables that control flow rates. More specifically, shared regional interest, which denotes that the two countries share at least one region in their top three for imports and exports, may improve diplomatic collaboration between the two countries. However, sharing common regional interests may also increase the probability of cyber conflict as the two countries compete for the same resources.

The diplomatic relationship stock also improves when two countries have shared dependencies or increased trade imports. A positive diplomatic relationship decreases the probability of cyber conflict. On the other hand, a diplomatic incident strains the diplomatic relationship, increasing the probability of cyber conflict.

Examining the trade relationship domain, we can see that trade imports influence and are influenced by the diplomatic relationship. Positive diplomatic relationships increase imports which in turn reinforce positive diplomatic relationships. Another reinforcing loop within our model exists between trade imports and regional interest. Increased trade imports may reflect an increasing interest in a trading partner's overall region, which could in turn increase imports. However, regional interest is also determined based on territory claims, wars occurring since 1980 and the presence of a diplomatic incident.

The loop between diplomatic relationships, trade imports and regional interests reveals by itself the complexity of connecting international relationships to possible cyber conflicts. For example, a positive diplomatic relationship directly decreases the probability of cyber conflict while indirectly increasing it through its positive influence on trade imports, which in turn increase regional interest.

It is interesting to observe that cyber capability is the only domain that directly affects the probability of a cyber attack without interacting with any other domain. As direct information about actual cyber capability is not usually made publicly available, we defined cyber capability as a combination of a country's total exports, which denotes that country's potential revenue to hire or train cyber attackers; the total number of citizens connected to the internet, which can be seen as a pool of talent from which a government can draw cyber attackers; and whether the country has demonstrated capability in past cyber incidents.

Figure 4. Probability of cyber conflict between USA and Iran one year before Stuxnet

Figure 5. Probability of cyber conflict between USA and Israel one year before Stuxnet

Figure 4 represents the output of our model when calculating the probability of cyber conflict between the United States and Iran for the one year period before the Stuxnet attack [1]. Our model currently only takes into account data from the year before a cyber attack. A year before Stuxnet, the probability of cyber conflict between the two countries was near 0.7, while for the same period the probability of cyber conflict between the United States and Israel was under 0.225, as shown in Figure 5.

V. CONCLUSIONS AND FURTHER WORK

Using a systems approach to better understand the shared international dependencies between nations, the potential state aggressor in a recent cyber attack may be identified. The system dynamics model put forth in this paper calculates the probability that two countries will engage in cyber conflict using publicly available information. After creating a dataset of 22 countries with military or civilian cyber capability, data on economic trade imports and diplomatic relationships were combined to identify dependencies, or countries upon which dependent countries rely for trade or military collaboration.

Nine case studies, in which the likely cyber combatant has been identified, were used to test the model. Initial results yielded a number of prior indicators of cyber conflict, such as dips in trade imports from future cyber combatants up to 2 years before a launched cyber attack.

In all case studies reviewed, the two countries imported heavily from overlapping regions. This indicates that countries competing for resources from the same regions are more likely to engage in cyber conflict to further their regional objectives. This could additionally explain why an aggressor might launch a cyber attack on an ally – as shared regional interests could contribute to a positive diplomatic relationship, they could by equal measure be justification for a cyber attack should the need arise. Other markers of regional interest, such as territory claims in the same region or recent wars fought in each other's regions, upwardly influence the probability that two countries will engage in cyber conflict, making regional interest the strongest determinant of cyber conflict of all variables in the model.

The earliest indicators of future cyber conflict are perceivably trade dips, which can occur up to 2 years before the launch of a cyber attack. While trade dips alone cannot indicate impending cyber conflict, when considered with other factors it is one of the strongest markers of a potential cyber combatant. Additionally, countries who do not share allies are slightly more likely to engage in cyber conflict.

Overall, cyber capability is difficult to establish from open-source data, but generally countries with greater numbers of internet users - as opposed to a greater proliferation of the internet - are more likely to initiate cyber conflict. This could have a link with greater population and their skills in the STEM domain (science, technology, engineering and maths) but that correlation needs to be more closely examined by future research (e.g. by looking more closely into offered programmes in computer science and IT, as well as cybersecurity).

In most cases of cyber conflict a deterioration of the diplomatic relationship between the two countries acts as a catalyst for the escalation to cyber conflict. This indicator is the 'smoking gun' leading to imminent cyber conflict.

The system dynamics model of cyber conflict opens up a number of avenues for further work, including further research on how cyber conflict relates to global economic crises and the use of fuzzy-logic programming to create a mathematical underpinning to the model.

Acknowledgment

This work has been supported in part by the European Union's Prevention of and Fight against Crime Programme "Illegal Use of Internet" - ISEC 2010 Action Grants (HOME/2010/ISEC/AG/INT/002) and also by the EPSRC-funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1) and its Industrial Partners.

References

[1] Farwell, J. P. and Rohozinski, R. "Stuxnet and the Future of Cyber War". *Survival: Global Politics and Strategy*, Volume 53, Issue 1, pp.23-40, 2011.

[2] Denning, D. E., *Information Warfare and Security*, New York: ACM Press Books, 1999.

[3] Rattray, G. J., *Strategic warfare in cyberspace*, Boston: Massachusetts Institute of Technology, 2001.

[4] Ryan, D. J., and Ryan, J. C. H., "Protecting the National Information Infrastructure Against Infowar". *Colloquy*, Vol. 17 (1), pp. 21-25, 1996.

[5] CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware, Centrum Wiskunde I& Informatica, [online] 7 June 2012, http://www.cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware (Accessed: 24 September 2012)

[6] Hinde, S., "Cyber-terrorism in context". *Computers I& Security*, Volume 22, Issue 3, pp.188-192, 2003.

[7] Lewis, J. A. and Timlin, K., "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization", UNIDIR *Cybersecurity and Cyberwarfare*, 2011.

[8] Anderson, D. et al, "Preliminary System Dynamics Maps of the Insider & Outsider Cyber-threat Problem", Proceedings of the 22nd International Conference of the System dynamics Society, pp. 25-29, 2004.

[9] Yang, S. C. and Y. L. Wang, "System Dynamics Based Insider Threats Modeling", *International Journal of Network Security and Its Applications*, Volume 3, Issue 3, pp. 1-14, 2011.

[10] Forrester, J. W., "Industrial Dynamics: A Major Breakthrough for Decision Makers", E.B. Roberts ed, *Harvard Business Review*, Volume 36, Issue 4, pp. 37-66, 1958.

[11] "South Korea blames North for bank and TV cyber-attacks", BBC News, [online] 10 April 2013, Available at: http://www.bbc.co.uk/news/technology-22092051 (Accessed: 10 April 2013)

[12] Nakashima, E. and Warrick, J., "Stuxnet was work of U.S. and Israeli experts, officials say", The Washington Post, [online] 2 June 2012, Available at: http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (Accessed 24 September 2012)

[13] Bencsáth, B. and Buttyán, L. and Félegyházi, M. and Pék, G., sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, [pdf] 2012, Available at: http://www.crysys.hu/publications/files/skywiper.pdf (Accessed: 24 September 2012)

[14] "Flame malware makers send 'suicide' code", BBC News, [online] 8 June 2012, Available at: http://www.bbc.co.uk/news/technology-18365844 (Accessed: 24 September 2012)

[15] Deibert, R. and Rohozinski, R., "Tracking GhostNet: Investivating a Cyber Espionage Network", Information Warfare Monitor, [online] 29 March 2009, Available at: http://www.f-secure.com/weblog/archives/ghostnet.pdf (Accessed: 24 September 2012)

[16] Krekel, B. and Adams, P. and Bakos, G.,"Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", US-China Economic and Security Review Commission, 7 March 2012.

[17] Miller, R. A. and Kuehl, D. T., "Cyberspace and the 'First Battle' in 21st-century War", *Defense Horizons*, Number 68, pp. 1-6, 2009.

[18] Falklands suffer the first Argentine attack of the 2010 cyber war, MercoPress, [online] 22 February 2010. Available at: http://en.mercopress.com/2010/02/22/falklands-suffer-the-first-argentine-attack-of-the-2010-cyber-war (Accessed: 24 September 2012).

[19] Haq, R., "Cyber Wars Across China, India and Pakistan". Haq's Musings, [online] 6 April 2010, Available at: http://www.riazhaq.com/2010/04/cyber-threats-across-china-india-and.html (Accessed: 24 September 2012)

[20] India and Pakistan in cyber war, Al Jazeera, [online] 4 December 2010, http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html, (Accessed: 24 September 2012)