Proxy Actors in the Cyber Domain: Implications for State Strategy

Jamie Collier

Abstract

States are increasingly compelled to work with non-state 'proxy' actors in the cyber domain. Within this nascent security domain, states have important strategic decisions to make, being able to use and interact with proxies in a diverse range of ways. This has led to a complex environment where the absence of doctrine has led to uncertainty going forward. This paper provides a taxonomy on the phenomenon of states using proxy actors in the cyber domain, outlining the proxy actors available to a state, the reasons proxy actors appeal, and the nature of state-proxy relations. It is argued that proxies are an increasingly important component of state strategy in the cyber domain. However, whilst proxy actors can bolster the capabilities of a state, they can also undermine a state's autonomy and security. States must therefore proceed with caution in working with a crucial, albeit risky, resource.

Introduction

States have long mobilised non-state actors for their own strategic gain. The trend of states using proxy actors has continued in the cyber domain, yet the phenomenon remains severely under-analysed.[i] This paper seeks to provide clarity on the issue by outlining a taxonomy of states' use of proxy actors in the cyber domain, the intention being to provide a framework for future analysis. A number of facets are explored, with focus on: the nature of proxy actors available to a state; the reasons why states turn to proxies; and the types of interaction that occur between states and proxies. In all of the aspects of state-proxy relations examined, a lack of uniformity is a consistent theme throughout.

The lack of uniformity in states' use of proxies highlights the complex challenges facing states at a tactical, operational,

i For papers that have considered this trend, see Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February 2011): 41–60; Christian Czosseck, "State Actors and Their Proxies in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 1–30; Florian Egloff, "Cybersecurity and the Age of Privateering: a Historical Analogy," *Cyber Studies Programme, Working Paper Series* 1, no. 1 (4 March 2015): 1–14.

Jamie Collier, "Proxy Actors in the Cyber Domain: Implications for State Strategy," *St Antony's International Review* 13. no. 1 (2017): 25-47

and strategic level: both as to how states can defend themselves against the proxy actors used by others and as to how states should mobilise proxies themselves. This paper will focus on the strategic or political aspects, discussing the high-level implications for states. The uptake in the use of proxies within the cyber domain represents a nascent security concern for policymakers. As conventional armed warfare is increasingly perceived as risky and expensive, the appeal of cyberattacks continues to grow in the gap between peace and all-out war. It is therefore important for international relations, as an academic discipline, to develop a full understanding of this emerging trend in the cyber domain.[ii] The academic community has largely neglected the strategic aspects of cyber security thus far.[1] To continue to do so risks undermining the role of international relations as an academic discipline that remains current and capable of informing policymakers.[2]

The findings of this paper show that states use proxies for different reasons. They may be used to avoid a state being implicated in an attack, or at least so that a state can reasonably claim plausible deniability. Alternatively, the use of proxies may reflect a lack of sophistication within a state's own capability, or demonstrate the advanced skill-set and capacity to innovate amongst non-state actors. Proxies are used by states to secure systems within their own borders, as well as to project power far beyond them.

A variety of proxy actors are available to states that include private sector firms, organized crime and hacker groups, and civilian-led militias. Proxies offer a breadth of functions including the coordination of cyberattacks, (e.g., denial of service attacks[iii] and advanced persistent threats[iv]), as well as less offensive assistance, such as providing states with expertise in defensive situations or access to threat intelligence. There is a spectrum of relationships that exist, with proxies ranging from recalcitrant to cooperative in their interaction with states.

Although many actors in the cyber domain are clearly either 'state' or 'non-state' actors, there are also several shades in between. The use of proxies therefore highlights a disconnect between the rigid distinctions deployed in international relations literature and the blurry distinctions observed empirically. Such

ii Although the nature and the level of threat at hand is contested, there is a consensus that further scholarly attention is required in order to develop understanding and enhance debate.

iii A denial of service attack is a malicious attempt to overwhelm a server or network with traffic in order to make it unavailable to users.

iv An advanced persistent threat is a system intrusion where an unauthorized user infiltrates a network, typically in order to continuously monitor and steal data.

an observation applies to proxy actors throughout the ages, yet is arguably more applicable to the cyber domain, given the greater ambiguity of actors' intentions and allegiances. Instead of a rigid separation between 'state' and 'non-state', state-proxy interactions should instead be conceptualized on a spectrum that captures the variety of relationships and levels of involvement between states and proxies that exist.

The discussion in this paper proceeds in five further sections.[v] The following section outlines the various types of proxy actors that exist. The focus then moves onto the reasons why proxies appeal to states, and states' interaction and relationships with proxy actors. The future outlook is also considered where it is argued that states' use of proxies is a trend set to continue for the foreseeable future. Finally, conclusions drawn from the discussion are outlined.

Proxy Actors in the Cyber Domain

This section provides an overview of the types of proxy actors that exist in the cyber domain. As shown below, a variety of proxy actors may be utilized by states.

Private Sector Firms

Many states maintain close relationships with private sector firms from a diverse range of industries. These firms offer several useful functions to states including security services, access to networks and intelligence, and knowledge of technical or system vulnerabilities.

Technology firms are frequently used by government intelligence agencies. The release of National Security Agency (NSA) documents by Edward Snowden has shown that many US technology companies, such as Facebook, Google, Apple, and Microsoft, have granted the NSA direct access to their servers under the government programme Planning Tool for Resource Integration, Synchronization, and Management (PRISM).[3]

Telecommunication firms have also assisted states in gathering intelligence, with BT, Vodafone, and Verizon all assisting GCHQ in accessing undersea cables.[4] Likewise, China enjoys a close relationship with many of its quasi-state businesses. Even Chinese firms that seem to have a high degree of autonomy, such as telecom firm Huawei, have been prevented by both Australia and the US from bidding on national contracts, due to fears that 'back doors'

v Many of the sections of this paper are based on the questions posed in Andrew Mumford, *Proxy Warfare* (Cambridge: Polity 2013).

will be installed, granting Chinese government officials access to sensitive systems and data.[5]

States also work with security companies. The UK collaborates with BAE Systems and QinetiQ in its Defence Cyber Protection Partnership.[vi] GCHQ clearly envisages outsourcing will continue in the long-term: in March 2010, GCHQ, along with private sector firms, purchased a new £40 million site in Cheltenham to house contractor staff.[6] Specialist cyber security firms are also a useful resource. There is close collaboration between Israel's military intelligence agency arm, Unit 8200, and Israeli private sector technology firms. Israel is even building a new 'cyber park' in Beer Sheva to encourage further tech start-ups and to develop relationships with private sector firms.[7]

The private sector supplies online services to states. Vupen, a French firm that sells knowledge of software vulnerabilities, claims to earn 80 percent of its revenue from the US government.[8] Italian-based Hacking Team has previously sold its surveillance technology, capable of infecting a target's device to steal files, read emails and record conversations, to a number of states with questionable human rights records, including Russia, Ethiopia, and Sudan.[9]

Militias and Civilian Volunteer Networks

States have also sought to utilize the expertise of civil society, engaging via civilian-based militias and volunteer networks. Although interaction with militias and volunteer networks is an often-favoured course of action taken by states, the organization of these groups varies significantly.

One often-adopted model is for states to house a volunteer cyber 'reserve unit' within their military reserve force. This has been implemented most successfully in Estonia where, as will be discussed in the following section, a number of national characteristics facilitate the participation of volunteers and civil society in the provision of national security. The Cyber Defence League (CDL)[vii] contains volunteers with a variety of specialties including computer science, cyber law, and crisis management strategy. The unit has a broad remit to provide assistance in developing cyber security practices and protecting

vi The Defence Cyber Protection Partnership is a partnership between the Government's primary defence departments, including GCHQ, the MOD and the Centre for the Protection of National Infrastructure (CPNI) along with thirteen private sector firms including BAE Systems, BT, Hewlett Packard, and QinetiQ amongst others participating.

vii The official name of the unit is the Defence League Cyber Unit, based in the Estonian Defence League. See http://www.kaitseliit.ee/en/cyber-unit.

critical national infrastructure. CDL members are organized on a voluntary basis and only paid when formally called up. They are also placed on standby in high-risk situations[viii] and have previously run exercises for cabinet ministers, ensuring interest and preparedness in cyber security amongst the highest levels of Estonian government.[10] Other states, such as the UK and the US, operate more constrained cyber reserves forces that are focused exclusively on the protection of military assets.

China provides a contrasting approach: students joining a technical university are required to participate in a militia as a de facto condition of enrolment.[11] This has given Beijing access to potentially thousands of highly-trained IT specialists that have expertise in software design, cyber security, and possibly even offensive espionage techniques.[ix] This also demonstrates the emerging relevance of non-traditional actors in the cyber domain, such as universities and technical academies that possess unique pools of knowledge and talent that states can tap into.

Militias have also provided a more offensive capability. The Iranian cyber-militia Iz a-Din al-Qassam Cyber Fighters launched cyberattacks on a number of US banks. The attacks were described as military grade and were considerably larger that the 2007 Russian attacks on Estonia. Such sophisticated capability for a civilian group seemed extremely unusual but was subsequently explained: it was later concluded that the group acted as a front organization to screen Iranian attacks on the US financial system.[12]

Hacker Groups

As states seek to enhance their offensive capability, cooperation with specialist hacker groups becomes an increasingly appealing option.

The Syrian Electronic Army (SEA) was established in 2011 and maintained close links to the Assad government, with several founding members having worked on previous government IT projects.[13] The SEA proved a useful tool for Assad in its early years with its activities ranging from producing a pro-Assad online narrative, to more destructive cyberattacks, and forms of online

viii For example, the CDL was on standby in the 2011 general election. Given that many Estonians vote online, an attack on the voting system during an election would be an obvious target for a potential aggressor.

ix The link between Chinese militias and offensive operations remains unclear. See Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: a Study of Chinese Information Warfare Militias," in *China and Cyber Security*, eds. Jon R Lindsay, Tai Ming Cheung, and Derek S Reveron (New York: Oxford University Press, 2015). 188–222.

exploitation directed at anti-Assad groups.[14]

Russia Business Network (RBN) is a cybercrime group which has been linked to a variety of criminal activities including botnet hire[x] and the production of malicious exploits and fake anti-malware. RBN has been suspected of involvement in the attack on Georgian websites at the same time Russia invaded the country.[15] Suspicions of RBN's links to the Kremlin are given additional credence by the fact that the creator of RBN is the nephew of a powerful and well-connected Russian politician.[16]

States also work with individual hackers directly. When the Chinese People's Liberation Army (PLA) discovered that Tan Dailin, a graduate student at Sichuan University, was attacking Japanese sites, he was subsequently invited to participate in a PLA cyber invasion methods training course. Dailin eventually formed his own group called Network Crack Program Hacker that went on to target US government agencies.[17]

Organized Crime Groups

States also collaborate with traditional organized crime groups that operated before criminal hacking opportunities arose. This is most clearly observed in Russia where hacking groups have grown out of mafia organizations. These mafia organizations are loosely connected to the government through a web of corruption, and indirect and intermittent ties to military and intelligence agencies.[18] Many of these mafia organizations, along with other hacking groups, conduct cybercrime operations worth billions of dollars each year. Given the low cost to the state, the Kremlin turns a blind eye when the victims are based outside Russian borders, whilst harshly punishing those that target Russian political actors.[19]

Along with the variety of proxy actors mentioned above, it is possible that other actors[xi] are used, or will be used in the future, by states including hacktivist[xii] groups, terrorist cells, private military contractors, and possibly even other nation states. It is also possible for the different classifications of actors outlined above to overlap: for example, a corporate employee serving in a

x A botnet is a large collection of computers that, unbeknown to their owners, have been set up to forward transmissions, including spam and viruses to other computers.

xi For an overview of the major actors in the cyber domain, see Gregory J. Rattray and Jason Healey, "Non-State Actors and Cyber Conflict," in *America's Cyber Future Security and Prosperity in the Information Age*, eds. Kristin M Lord and Travis Sharp (2011), 65–86.

xii Hacktivism is used to describe many forms of online activism, where computers are used to promote a political agenda or principles such as free speech or human rights.

volunteer defence unit. Having established that states use, or are able to act through, a wide range of proxies in the cyber domain, it is now appropriate to explain why the use of these actors has particular appeal to states.

The Appeal of Proxy Actors

Proxies in the cyber domain appeal to states for a variety of reasons. In a broader context, proxy actors have appealed to states throughout history. For example, the Roman, Turkish, and European colonial empires all used conquered peoples to assist their expansion, and volunteers were used on a large scale during the Sino-Japanese and Spanish civil wars.[20] Indeed, parallels have even been drawn convincingly between states' use of proxies in the cyber domain today and states' mobilisation of navies, mercantile companies, pirates and privateers during the sixteenth and seventeenth century.[21]

This historically ubiquitous trend[22] raises questions over the significance of the appeal of proxies in the cyber domain: specifically, whether states' use of proxies represents an altogether new development, or merely a continuation of an existing trend in a contemporary context.

The argument that proxy actors are an important component of state strategy and therefore appeal to states is contentious. As proxy actors outside of the cyber domain have become less centralized and formalized, they have become increasingly likely to defect against their state sponsors, highlighting the risk of blowback.[23] Further, previous literature has made convincing arguments that states remain the dominant actors in the cyber domain, given their unparalleled ability to inflict physical damage.[24] For example, the most physically destructive cyberattack, Stuxnet, which compromised an Iranian nuclear subterfuge, was orchestrated by the US and Israel. Such state-centric arguments may therefore dismiss the appeal or impact of proxy actors. Whilst it is not disputed that states remain the most capable actors in inflicting physical damage in the cyber domain, it is argued that it is wholly inappropriate to measure power and capability solely through the lens of physical harm. The cyber domain requires a conceptual rethink towards notions of security. This is in order to include the vast array of types of damage such as economic, psychological, and cultural. When consideration is given to this full spectrum of activities in the cyber domain (ranging from financial crime and espionage, to acts of political suppression and the distribution of propaganda) the landscape is drastically varied with states being merely one of a number of actors. When cyber power is considered in this broader sense, traditional international relations

approaches (such as realist theories that stress the power of nation-states) offer a perspective that is markedly less relevant. Instead, the growing popularity of proxies demonstrates the importance of a diverse range of actors in the cyber domain.

This paper now turns to examine the reasons why states use proxies in the cyber domain.

Power Diffusion

The most significant reason that the use of proxies appeals is due to an ongoing process of power diffusion in the cyber domain.[25] The power diffusion process involves two interrelated trends: nation-states struggling to adapt to the challenges in the cyber domain and the emergence of a number of non-state actors.

Certain characteristics of the cyber domain have challenged the traditional monopoly held by states on the provision of security. There is currently a severe lack of skilled workers in a number of technical disciplines, such as computer science, cyber security, and software engineering. Therefore, those with such skills can command high salaries that governments struggle to afford.[26] This is a worry for the UK intelligence agency GCHQ, with the parliamentary Intelligence and Security Committee recently raising concerns over the agency's inability to retain a suitable cadre of internet specialists to respond to the threat at hand. Many GCHQ employees are able to earn over three times their salary when they move to technology firms such as Google, Microsoft, and Apple.[27] Such an exodus has led to suggestions that GCHQ will have to alter its strategic thinking in the future.[xiii] Further, the underlying infrastructure of the cyber domain is largely outside state control—for example, it has previously been estimated that 98 percent of US government communications, including classified communications, travel over civilian owned and operated networks and systems.[28]

Government and regulatory timelines have struggled to keep up with the fast pace of technological change: US Congress failed to pass a single piece of major cyber security legislation between 2002 and 2014, and it took the US Federal Risk and Authorisation Management Program six months to approve its first contractor. Although six months was regarded as fast within government, given the relevant

xiii Former GCHQ Director Iain Lobban suggested that the agency might have to reconsider its requirement that it only hires British nationals (see ibid). It has also been proposed that the agency creates programs that seek to attract employees for a short-term period (around two years) before going on to other careers. See Oliver Wright, "GCHQ's 'Spook First' Programme to Train Britain's Most Talented Tech Entrepreneurs," *The Independent* (1 January2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/gchqs-spook-first-programme-to-train-britains-most-talented-tech-entrepreneurs-9953516.html.

bureaucratic hurdles to be negotiated, the pace was regarded as sluggish amongst the wider cyber security community.[29]

Characteristics of the cyber domain have also empowered non-state actors. Unlike traditional military domains, the skills required to succeed in the cyber domain are entrenched in the civilian sector. The reduced cost of online technology has made it possible for a variety of actors to distribute large quantities of information. Reduced costs also lower the barriers to entry, enabling new actors and increasing the potential for civil-military integration. Unlike the significant capital required to build fighter jets and naval vessels, sophisticated tools in the cyber domain can be developed by small businesses and start-ups.[30] Further, given that barriers to entry are particularly low, non-state actors have little to lose from exit and re-entry, making them inherently more flexible and adaptable to change when compared to states.[31] Given these advantages held by non-state actors, states have a natural incentive to work alongside them.

The global scale of the cyber domain can also naturally benefit multinational corporations. Technology monopolies possess a global outreach to the envy of even well-resourced intelligence agencies. For example, Cisco's dominance in the router market allows the firm to see and analyse a significant proportion of global Internet traffic. Google and Microsoft's respective dominance in the search engine and desktop operating system markets are likely to yield similar levels of access. In addition, software exploit and vulnerability markets[xiv] offer a valuable resource for states that are able to access a global marketplace, as opposed to the capability of government employees alone.

Since World War II, the most powerful states have rarely used proxies to compensate for deficiencies in national capabilities. In the Cold War, superpowers used proxies not due to weaknesses in their own militaries, but, because direct war against another nuclear power was deemed too risky. Today, the leading Western powers use proxies due to a realization that direct wars represent a significant political and electoral risk. Since the electoral backlash against the War on Terror, states such as the US and UK are learning that many of their citizens do not have the appetite, nor are willing to foot the bill, for protracted military campaigns.[32] The cyber domain is perhaps unique, as a contemporary domain, with non-state actors possessing some of the finest minds, most sophisticated infrastructure and advanced capability.

xiv For further information on these markets, see Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data," RAND (14 March 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Plausible Deniability

Plausible deniability is frequently referred to as a reason why proxies are used in the cyber domain, particularly for offensive purposes. This is consistent with how proxies have been used in the past. As discussed above, the use of proxies appealed in the Cold War era when direct war against a nuclear power was considered too risky. Yet, if states attacked via proxies, they could claim plausible deniability, reducing the risk of retaliation. Likewise, proxies in the cyber domain are also able to muddle blame attribution.[33] For example, before and during the Russian invasion of Georgia in 2008, Russian cyber militias disabled key portions of Georgia's communication system. It made sense for attacks to be conducted by militias as opposed to state-owned actors—in order to compromise Georgian systems, civilian systems in third-party states also needed to be attacked. Had a Russian state actor been implicated, the attack would have violated laws of armed conflict regarding the principle of distinction between military and civilian targets.[34] Further, assuming the Russian government was involved in the 2007 Estonian cyberattacks conducted by patriotic hackers, the Kremlin was able to respond whilst circumventing accountability and avoiding at least some of the diplomatic costs of direct action. This illustrates the argument that it is more difficult to deter a state from attacking in the first place if it is doing so under the cover of a proxy.

Although the conventional wisdom that proxies are used to allow states to claim plausible deniability certainly applies in the cyber domain, the benefits have been overemphasised for two reasons. First, as previously discussed, circumstantial evidence is increasingly used in the attribution process. For example, the 2007 Estonian cyberattack was in response to a Russian war memorial being relocated from the centre of Tallinn, the Estonian capital. This political context went some way to implicating Russia in the cyberattacks. Healey has argued that states should more readily place blame on other states for cyberattacks that originate from their territory.[35] As the use of circumstantial evidence in the attribution process gains traction, the marginal benefit of using proxies is reduced—especially for proxies known to maintain a close relationship with a particular government. Second, the supposed difficulties in attribution are themselves contested. Rid and Buchanan have argued convincingly that, contrary to the arguments that the state has been in perpetual decline in the cyber domain, sophisticated state agencies, in fact, have the necessary resources to attribute actors with a high degree of certainty.[36] If such agencies can attribute the perpetrators of cyberattacks with confidence, establishing a link between proxies and their state sponsors would also appear feasible. Conversely, there is

little incentive for an aggressor state to act via a proxy actor against targets that do not possess sophisticated attribution capabilities: if an aggressor state can conceal its identity independently, working with proxies only entails additional risk: both through the loss of state autonomy in the operation of an attack, and the danger that such proxy actors will reveal information about their state sponsor, either advertently or inadvertently. The appeal of proxies, for the purposes of an aggressor state being able to claim plausible deniability, therefore amounts to situations in which a target state is able to attribute an attack to an actor, but unable to prove a link between such an actor and a state sponsor. Although plausible deniability remains a valid reason why proxies appeal to states, the real benefit is considerably more marginal than often claimed, highlighting the fact that other factors are at play in explaining the appeal of proxies.

Cost Saving

Proxies have historically been used by a state to reduce costs, especially when a state lacks task-specific knowledge and expertise. Delegation to proxies also allows states to benefit from the efficiency gains of specialization.[37] Outsourcing is a popular model in the cyber domain, particularly in certain Western states such as the US and UK.[38] A state often only requires assistance from proxies on a short-term basis. By outsourcing, a state is able to access expertise and capability as and when it is required without the additional costs associated with permanent employees such as pension plans, sick leave, and training. The prospect of a return on investment in training is particularly low: training for technical jobs can take a long time and as agencies such as GCHQ have found, many employees, once trained, will only stay for a short period before going to work for the private sector. Further, as previously discussed, power diffusion has lowered the barriers to entry in the cyber domain for a number of actors. With many private sector firms able to bid for national contracts, costs should theoretically be driven down.

Avoidance of Direct Intervention

Proxies often provide a convenient tool for states to pursue their foreign policy agenda. This can be observed through US interaction with proxies. Although eager to assist anti-Assad rebels, the US was reluctant to intervene directly in Syria. Instead, the US diverted financial aid to provide technical assistance and equipment as well as training for networks of Syrian journalists, bloggers, and cyber-activists, to enable them to document and

disseminate information on developments in Syria, and to protect Syrian activists.[39] In addition, the US Office of Foreign Asset Control directed American technology company Network Solutions LLC to seize more than seven hundred domain names associated with the Assad government, forcing the regime to adjust its online presence.[40] This is consistent with US support for political dissent in the past. The US government has previously asked Twitter to maintain its service in Iran in order to help facilitate the organization of demonstrations.[41]

Reinforce State Authority

Sometimes, states' use of proxies is significantly shaped by broader strategic goals. China, which is less expansionist than its Western counterparts, is more concerned with maintaining domestic order. It has previously been argued that China has encouraged China-based hackers to attack others, in part to keep them from targeting Chinese assets or undermining the Chinese government.[42]

Russia appears willing to turn a blind eye to cyberattacks that target victims abroad, but will harshly punish citizens that attack Russian political figures.[43] The Kremlin also uses proxies in its propaganda campaign, adding hundreds of operatives to counter the Western narrative of its invasion of Ukraine. Internet 'trolls' are employed by Internet Research, a Russian firm financed by a holding company headed by a friend of Putin.[44] The online operatives work twelve-hour shifts, using social media accounts to spread propaganda as well as leaving comments on various websites and videos online.[45] As previously discussed, the Syrian Electronic Army, established by the Assad government, has conducted similar activities online.

The suggestion that states use proxies to reinforce state authority might seem to contravene earlier arguments about power diffusion (where states turn to proxies due to deficiencies in their own capability). Yet these two trends do co-exist. While the power diffusion thesis asserts that states' cyber capabilities are relatively less powerful given the empowerment of non-state actors, the point made here relates to how states can then utilize the capabilities of non-state actors in various ways to either discourage dissent or to actively shape narratives that promote the state.

State Security

Proxies are vital in the provision of state security. As well as using contractors to protect government infrastructure, states have also

established information-sharing partnerships where states and private sector firms share information in a mutually beneficial arrangement. However, state power is constrained when the private sector owns large sections of critical national infrastructure. In states such as the UK, the government struggles to regulate these firms partly due to the strong property laws that protect private sector firms from state interference. Nonetheless, states are eager to work closely with the owners of critical national infrastructure to ensure adequate security standards are maintained.

Likewise, proxies are essential in the provision of intelligence for a state. Documents leaked by Edward Snowden show that organizations such as the NSA and GCHQ work closely with a number of private sector firms. States are also the majority customer in the global surveillance products market, estimated to be worth $5 billion. This involves the selling of tracking, monitoring, and eavesdropping technology. Whilst these products can prove vital tools for national security, they have also been used to support despotic regimes and to prevent peaceful political dissent.[xv]

National and Cultural Characteristics

States often work with proxies due to cultural connections. Estonia provides a good example where the participation of civilians in groups such as the Cyber Defence League grows out of national characteristics.[xvi] Estonia operates a Total Defence model where it is expected, given the small size of the state, that civilians contribute to Estonian national security efforts.[xvii] In addition, having only regained independence from the Soviet Union in 1991, and with Russia still posing a viable threat, there is a deep sense of patriotism and a recognition that Estonian citizens must unite in order to secure their borders. With technology having played a decisive role in Estonia overcoming the legacy of the Soviet Union,[46] there is also a close association between cyber security and national security more broadly. A combination of these cultural, political, and historical factors mean that it is natural for the Estonian government to utilize willing civilian-based groups in the cyber domain.

xv Sari Horwitz, Shyamantha Asokan, and Julie Tate, "Trade in Surveillance Technology Raises Worries," *The Washington Post* (1 December 2011), https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html.

xvi Jamie Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," eds. Mariarosaria Taddeo and Ludovica Glorioso, *Ethics and Policies for Cyber Operations* (Cham: Springer, 2016).

xvii Ants Laaneots, "The Estonian Defence Forces – 2000," *Baltic Defence Review* 1, no. 1 (1999): 1–7; Milton P Davis, "An Historical and Political Overview of the Reserve and Guard Forces in the Nordic Countries," *Baltic Security Defence Review* 10 (18 August 2008): 171–201.

Proxies appeal to weak or small states in unique ways. Cyber militias in Estonia, Latvia, Lithuania, Georgia, and Kyrgyzstan have all threatened to retaliate against future Russian cyber- or kinetic attacks.[47] As previously discussed, Iran has also been able to use militias as an effective tool to attack US financial institutions. Whilst weaker states are typically unable to pose a substantial kinetic threat to stronger states, they are potentially better placed to retaliate in the cyber domain given the low barriers to entry. Although cyberattacks have failed to prove as destructive as kinetic weapons,[48] proxies may nonetheless help weaker states balance the odds against more powerful adversaries.

As demonstrated above, the use of proxies appeals to states for a number of reasons. This leads to challenges in interpreting and understanding the phenomenon. The logic that the incidence of cyberattacks would lead to a nuclear retaliation seems dubious, casting aside Cold War paradigms. More recently, the War on Terror has left a legacy of a public distaste for direct wars in the West. Whilst this logic may explain why cyberattacks would be used (instead of direct war), they do not explain why they would be conducted via a proxy: cyberattacks are not as politically sensitive as direct war so there is arguably less need to conceal actions via proxies. Likewise, proxies with extensive local knowledge and experience have previously appealed to states that do not possess the same level of expertise.[49] Yet, such local knowledge is not a prerequisite for successful attacks in the cyber domain.

The use of proxies in the cyber domain is a novel phenomenon. Previous understanding on the use of proxies has not had to account for aspects of the cyber domain, such as the ongoing power diffusion process where even great powers use proxies due to deficiencies in their own capability. Thus, it is difficult to interpret and understand the use of proxies given the diversity in their use—ranging from political hacktivists, to criminal syndicates, to civilian militias.

State Interaction with Proxy Actors

Whilst the use of proxies appeals for a number of reasons as discussed above, states must still understand how to develop relationships with proxies in order to best garner their assistance and cooperation. Similar to the conclusions in previous sections, on this matter there is a lack of uniformity in opinions on the most suitable approach, with a variety of strategies currently exhibited by states.

States' interaction with proxies comprises two dimensions: states must decide on the type of relationships to form with proxy actors, as well as establish the degree of state involvement in the activities of a proxy.

State-proxy Relationships

A variety of relationships exist between states and their proxies, ranging from active cooperation to coercion. There is even significant variety within just one state-proxy relationship: the Chinese government has interacted with militias in at least four different forms including formal procurement relationships, formal outsourcing, transactional and coerced outsourcing as well as operational outsourcing.[50]

Certain proxies are reluctant to assist states. States are therefore required to coerce some actors in order to gain their assistance. The US used coercive tactics in its pursuit of the hacking group Lulzsec. Lulzsec grew out of the group Anonymous and conducted a number of disruptive attacks. Lulzsec also claimed responsibility for an attack on the public-facing website of the US Central Intelligence Agency (CIA).[51] Hector Monsegue (known by the online pseudonym Sabu) was one of the co-founders of the group. When Monsegue was caught by the FBI and threatened with a heavy jail sentence, he became an FBI informant, working with the agency to identify fellow hackers and help overthrow the group.[52]

Other proxies maintain inconsistent relationships with states, perhaps only working together when there is a mutual interest. The Syrian Electronic Army (SEA) has maintained an episodic relationship with the Assad government. Whilst the SEA started out as a state-sponsored group, when the Assad government became further besieged with domestic turmoil and civil war, the SEA changed its methods and membership. It gradually became more of a loose hacking collective, as opposed to a state-sponsored brigade.[53] The SEA maintained links with Assad, yet as the group was not an official government entity, the relationship between Assad and the group began to wane.

States also work with proxies through more mutually beneficial agreements. Outsourcing is one area where proxies work with states for financial reward. For example, in 2009/10, GCHQ spent £43.1 million on contractors.[54] In Israel, the Office of the Chief Scientist based in the Ministry of Economy dispenses risk-free government loans to technology start-ups and demonstrates that financial assistance can be used to foster close relationships with private sector firms.[55] Other public-private partnership agreements are voluntary and perhaps begin to move away from a state-proxy dynamic. For example, the UK's Cyber Security Information Sharing Partnership (CISP) acts as a portal where both private sector firms and government agencies can view and exchange information on threats and vulnerabilities in real time.[56]

Other proxies enjoy close relationships with states. In 2010,

when Google withdrew its business from China, the firm worked closely with the US government, informing them before their public announcement. The US government benefitted from Google's withdrawal, using the incident to push for the adoption of Internet norms supported by the US.[57] The 2014 Sony data breach demonstrates how the concerns of a non-state actor can spill onto government agendas. Whilst the breach occurred at a private sector media company, the event soon became embroiled in a broader narrative as an attack on US First Amendment Rights of free speech.[58]

Some actors are so closely aligned with state interests that the interaction between the two is paradoxically minimal. Parallels have been drawn between ideologically motivated proxies and the political action committees (PACs) that operate in US election campaigns.[59] Proxies have defended the interests of their state with minimal coordination, much like a PAC that directs efforts towards a political campaign without working directly for a candidate. Russian and Chinese citizens regularly act in the interests of the state without direct coordination, often to allow the state to maximise its ability to claim plausible deniability. With these proxy actors proactive in defending state interests, it is clear that some proxies are motivated predominantly by ideology and loyalty to a state, as opposed to financial gain.[60]

States therefore have a number of tools available to them in interacting with proxies (such as regulatory powers, law enforcement, its own purchasing power, etc.). Yet, the relationships states form are often linked to broader political, cultural, and historical factors. For example, Russia has been able to extend its links with criminal groups into the cyber domain. But, for Western states, interaction with criminal groups is politically unviable; they have alternatively developed close relationships with predominantly private sector firms. As shown in the Assad regime's interaction with the Syrian Electronic Army, states may look to create or instigate the establishment of proxy groups when no current state-proxy relationships exist.

Whilst states' relationships with proxy actors are largely dictated by broader political, cultural, and historic variables, states potentially have more leverage over their level of involvement in the activities of proxy actors. As demonstrated below, in addition to the different categories of relationship that exist between states and proxy actors, the level of state involvement in the activities of proxy actors also varies significantly.[xviii]

Level of State Involvement

xviii For detail on spectrum of state involvement in cyberattacks see Healey, "Beyond Attribution"; Jason Rivera, "Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk," 7–24.

When proxies act in the state's interest without direct coordination, the state has, by definition, minimal involvement. States may simply be aware of the actions of other actors but choose to ignore them (or at least do nothing to prevent them). This possibly occurred in the 2007 cyberattacks on Estonia. Alternatively, proxies may be gently encouraged by states. Third parties will still conduct the attack, but their actions are supported by national governments as a matter of policy. For example, in 2007 Iran created the Basij Cyber Council to organize Iranian civilian hackers under the supervision of the Iranian Revolutionary Guard Corps.[61]

Further up the spectrum of involvement, actions may be state-ordered where national governments direct proxies to attack on their behalf. States can get further involved in the actions of proxies through state-rogue-conducted attacks, where supposedly rogue government departments conduct cyberattacks. For example, in 1999 after the accidental bombing of the Chinese embassy in Belgrade, rogue hackers from a number of government departments in anti-Western states such as Russia, Latvia, Lithuania, and Serbia conducted anti-NATO cyberattacks.[62]

The line between states and their proxies becomes increasingly blurred in state-integrated actions. This may occur when governments integrate both government departments and external proxies in order to conduct cyberattacks.

The Continuing Appeal of Proxy Actors and Future Implications

Although the difficulty in predicting the future of conflict is acknowledged,[63] state use of proxies appears to be a trend that is set to continue.

Crucially, many of the reasons proxies appeal in the current environment are likely to endure in the future. Given commercial incentives, the private sector will continue to invest in research and offer an advanced capability. Businesses and people are being attacked on a regular basis in the cyber domain, creating a significant private market for security solutions that has not existed in other security domains. Likewise, the use of organized criminal gangs and hackers will continue to enable states to act in ways perceived as illegitimate by the international community. While it is therefore likely that states will continue to use proxies, it is less clear how international relations literature will interpret their role. One school of thought would present the phenomenon as an example of state power, with proxies acting as an extension of a state's capability. Conversely, it could be argued that proxy actors are often used precisely because of the deficiencies in a government's own capability. States are thus

partly dependent on actors that are not compelled to work with them, thus highlighting the frailties of state power.

It is acknowledged that there are reasons why the use of proxies may decline in popularity. Many states use proxies due to the current skills gap that may not continue in the future as education initiatives in technical disciplines continue to develop. Further, whilst states are able to enhance their capability through the use of proxies, they potentially forfeit a degree of their own autonomy and control in the process. The Syrian Electronic Army's turbulent relationship with the Assad regime shows that state-proxy relations can prove unstable. Further, for states to convincingly claim plausible deniability, they must reduce evidence of state control. However, reducing evidence of state control often requires reducing actual state control.[64] For states to viably claim plausible deniability in their association with criminal groups, they will have to tolerate a degree of cybercrime that is damaging to their economy and which threatens state interests. Whilst the benefits of using these groups currently outweigh such costs, states may increasingly search for less harmful solutions.

Implications for Proxy Actors

Proxy actors are faced with ethical and foreign policy decisions, previously outside their purview. For example, Google's withdrawal from China and collaboration with US intelligence agencies demonstrates that their actions increasingly have political implications. Further, whilst some proxies remain loyal to specific states, others have chosen to work with a range of states. For example, Italy-based Hacking Team has been willing to sell its spying tools to a variety of states with questionable human rights records such as Russia, Ethiopia and Sudan.[65] Whilst a UN arms embargo would prevent firms from selling weapons to such states, as spying tools do not count as weapons, private sector firms are currently able to sell such products and services with fewer restrictions.[66]

Private sector firms are increasingly faced with a dilemma in working with states. States represent a potentially valuable client base and it is vital for firms to retain their business. However, working with states, or even just appearing to work with states, can lead to mistrust amongst other states and consumers. For example, there was clear public anger when the NSA documents leaked by Edward Snowden revealed technology firms had worked closely with intelligence agencies. Likewise, although respected in the cyber security industry, many Western organizations are wary of cyber security firm Kaspersky, given alleged ties with the Kremlin. Even if such allegations are unfair, it is often perceptions that matter more than facts.

Given this tension, states may seek to portray "separation theatre"[67] where efforts are made to create a public perception that firms are distancing themselves from states, whilst in fact maintaining close relations behind closed doors. This process is arguably already occurring: firms such as Google and Apple have worked hard to distance themselves from the US government since the Snowden leaks, yet the measures they have implemented have had arguably only a limited effect. For example, whilst Apple now encrypts devices by default, there are a number of ways intelligence agencies such as the NSA can potentially still access data.[68]

There is also a danger that the relationships between proxies and states, or at least the perceptions of such relationships, will foster mistrust. Iran has accused the firm Siemens of colluding with the US and Israel in creating the Stuxnet virus that sabotaged an Iranian nuclear centrifuge that ran Siemens software, despite the lack of evidence of Siemens involvement. States could therefore become increasingly inward looking, working as much as possible with domestically based actors (e.g. Iran working predominantly with Iranian firms, Brazil with Brazilian firms, etc.). Whilst many of these non-state actors are responsible for the extensive globalization process brought by the digital sector, they themselves risk becoming increasingly isolated in the world.

Conclusion

In examining states' use of proxies in the cyber domain, there is wide variation on a number of fronts. Many different proxy actors exist; proxies appeal for a variety of different reasons; and there is a spectrum of state involvement in the activities of their chosen proxies. This lack of uniformity is largely due to the different strategies and objectives being pursued by states. However, it also reflects the range of functions proxies can offer, ranging from offensive cyberattacks, to the provision of cyber security solutions.

It is argued that the use of proxies will continue to hold appeal in the future as the reasons proxies are used today are likely to remain in the future. Further, as the barriers to entry in the cyber domain remain low, new actors will continue to develop and become viable proxies for states.

Given that this is a trend set to continue, there are challenges going forward—both for states and proxy actors. There remain open questions on how states can protect themselves from the aggressive actions of proxies mobilised by other states. States must optimise their own strategy by establishing what proxies are available to them and which actors are most appropriate to work with—taking into account their capability and reliability. The lack of uniformity that

currently exists reflects the sheer breadth of different strategies being pursued by states. Yet, it remains unclear which strategies are the most successful. For example, whilst the proxies with the most advanced capability are arguably Western private sector firms, they are much more constrained, in offensive terms, at a political level when compared to organized crime and hacker groups whose relationship with a state is perhaps more ambiguous, enabling more aggressive action to take place.

Theoretical understanding needs to be developed in order to explain the reasons why proxies appeal in the cyber domain. Wider examples of states using proxies outside the cyber domain as well as existing international relations theory that has sought to explain this trend are both useful indicators that can provide lessons, at a strategic level, in the cyber domain. Yet, wider examples and previous theory do not fully capture the dynamics of the cyber domain. Some of the historical motivations for using proxies do not translate neatly into the cyber domain. Conversely, there are also more novel reasons why the use of proxies appeals specifically in the cyber domain. For international relations theory to remain relevant and capable of informing policymakers, greater understanding of states' use of proxies in the cyber domain needs to be developed. This may take the form of analysis regarding the costs and benefits associated with working with proxies or examining how traditional international relations concepts (such as deterrence or signalling) apply to proxy actors.

Given the importance of a range of actors, traditional ideas of the state's monopoly on the provision of security need to be rethought. The appeal of proxies also demonstrates that it is wholly inappropriate to seek to militarize the cyber domain, with many of the skills and capability entrenched in civil society. With a spectrum of relationships and multiple levels of state involvement in the actions of proxies, it is also vital to examine state-proxy dynamics with sufficient nuance. Crucially, whilst states are compelled to work with a range of non-state actors in the cyber domain, in doing so, the boundaries of statehood become increasingly blurred.

Notes

1 Adam P. Liff, "Cyberwar: a New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 401–28.
2 Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (October 2013): 7–40.
3 "NSA Snooping: Facebook Reveals Details of Data Requests," *BBC News* (15 June 2013), http://www.bbc.co.uk/news/world-22916329.

4 James Ball, Luke Harding, and Juliette Garside, "BT and Vodafone Among Telecoms Companies Passing Details to GCHQ," *The Guardian* (2 August 2013), http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.
5 Jon R Lindsay, Tai Ming Cheung, and Derek S Reveron, *China and Cyber Security* (New York: Oxford University Press, 2015).
6 Malcolm Rifkind, "Intelligence and Security Committee Annual Report 2010-2011" (7 June 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211561/isc-annualreport1011.pdf.
7 John Reed, "Unit 8200: Israel's Cyber Spy Agency," *Financial Times* (12 July 2015).
8 Czosseck, "State Actors and Their Proxies in Cyberspace," 1–30.
9 Cora Currier and Morgan Marquis-Boire, "A Detailed Look at Hacking Team's Emails About Its Repressive Clients," *The Intercept* (7 July 2015), https://firstlook.org/theintercept/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.
10 Sharon L Cardash, Frank J Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: a Model for the United States? *Studies in Conflict & Terrorism* 36, no. 9 (September 2013): 777–787.
11 Klimburg, "Mobilising Cyber Power," 41–60.
12 Richard B Andres, "Cyber-Gang Warfare," *Foreign Policy* (12 February 2013), http://foreignpolicy.com/2013/02/12/cyber-gang-warfare/.
13 Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," *Comparative Strategy* 34, no. 2 (15 May 2015): 133–48.
14 Grohe, "The Cyber Dimensions."
15 Greg Keizer, "Cyberattacks Knock Out Georgia's Internet Presence," *Computer World* (11 August 2008), http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html.
16 Peter Warren, "Hunt for Russia's Web Criminals," *The Guardian* (15 November 2007), http://www.theguardian.com/technology/2007/nov/15/news.crime.
17 Klimburg, "Mobilising Cyber Power," 41–60.
18 Andres, "Cyber-Gang Warfare."
19 Andres, "Cyber-Gang Warfare."
20 Towle, "The Strategy of War by Proxy," 21–26.
21 Egloff, "Cybersecurity and the Age of Privateering: a Historical Analogy," 1–14.
22 Mumford, *Proxy Warfare*.
23 Milos Popovic, "Fragile Proxies: Explaining Rebel Defection against Their State Sponsors," *Terrorism and Political Violence* (forthcoming).
24 Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015).
25 Nye, *The Future of Power*, 113–151.
26 Czosseck, "State Actors and Their Proxies in Cyberspace," 1–30.
27 Duncan Gardham, "Whizz Kids Deserting the Spy World as Threat of Attacks Increases," *The Telegraph* (13 July 2011), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8635959/Whizz-kids-deserting-the-spy-world-as-threat-of-attacks-increases.html.
28 Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014).
29 Singer, *Cybersecurity and Cyberwar*.
30 Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity: a Study of Chinese Information Warfare Militias," 188–222.
31 Nye, *The Future of Power*, 113–151.
32 Mumford, *Proxy Warfare*.
33 Andres, "Cyber-Gang Warfare."
34 Andres, "Cyber-Gang Warfare."

35 Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks."
36 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1 (25 April 2014): 4–37.
37 Idean Salehyan, "The Delegation of War to Rebel Organizations'" *Journal of Conflict Resolution* 54, no. 3 (8 June 2010): 493–515.
38 Alastair Stevenson, "GCHQ and NSA Outsourcing Cyber Security Tasks to Third-Party Vendors," *V3* (24 March 2013), http://www.v3.co.uk/v3-uk/news/2296504/gchq-and-nsa-outsourcing-cyber-security-tasks-to-third-party-vendors.
39 Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," 133–48.
40 Brian Krebs, "Trade Sanctions Cited in Hundreds of Syrian Domain Seizures," *Krebs on Security* (8 May 2013), http://krebsonsecurity.com/2013/05/trade-sanctions-cited-in-hundreds-of-syrian-domain-seizures/.
41 Nye, *The Future of Power*, 113–51.
42 Klimburg, "Mobilising Cyber Power," 41–60.
43 Andres, "Cyber-Gang Warfare."
44 Adrian Chen, "The Agency," *New York Times* (2 June 2015), http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.
45 Chen, "Agency."
46 "How Did Estonia Become a Leader in Technology?" *The Economist*, (30 July 2013).
47 Andres, "Cyber-Gang Warfare."
48 Valeriano, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*; Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst 2013).
49 Salehyan, "The Delegation of War to Rebel Organizations," 493–515.
50 Sheldon, "Civil-Military Integration and Cybersecurity: a Study of Chinese Information Warfare Militias," 188–222.
51 "LulzSec Hackers Claim CIA Website Shutdown," *BBC News* (16 June 2011), http://www.bbc.co.uk/news/technology-13787229.
52 Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: the Many Faces of Anonymous* (London: Verso 2014); Parmy Olson, *We Are Anonymous*, (London: William Heinemann, 2013).
53 Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," 133–48.
54 Gardham, "Whizz Kids Deserting the Spy World as Threat of Attacks Increases."
55 Reed, "Unit 8200: Israel's Cyber Spy Agency."
56 Tim Ring, "Threat Intelligence: Why People Don't Share," *Computer Fraud & Security Bulletin* 3 (11 March 2014): 5–9.
57 Nye, *The Future of Power*, 140–142.
58 Ellen Nakashima, "Why the Sony hack drew an unprecedented U.S. response against North Korea" (15 January 2015), https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?utm_term=.9ad1a8a61c6c.
59 Peter Suciu, "How Hackers Work Like a PAC."
60 Suciu, "How Hackers Work."
61 Rivera, "Achieving Cyberdeterrence," 7–24.
62 Jonathan Diamond, "Early Patriotic Hacking," in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, ed. Jason Healey (Vienna, VA: Cyber Conflict Studies Association 2013), 138–39; Rivera, "Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk," 7–24.
63 Robert A. Johnson, "Predicting Future War," *Parameters* 44, no. 1 (25 April 2014), 65–76.
64 Andres, "Cyber-Gang Warfare."

65 Currier, "A Detailed Look at Hacking Team's Emails About Its Repressive Clients."
66 Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," (6 July 2015), http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.
67 Jamie Collier, "Public-Private Partnerships in the Cyber Domain: Implications for Globalisation," *Cyber Security Relations* (22 July 2015), http://www.cybersecurityrelations.com/blog/public-private-partnerships-in-the-cyber-domain.
68 Andrew Zonenberg, "Why Apple's iPhone Encryption Won't Stop NSA (or Any Other Intelligence Agency)," *Silicon Exposed* (4 October 2014), http://siliconexposed.blogspot.co.uk/2014/10/why-apples-iphone-encryption-wont-stop.html.