Brazil struggles with effective cyber-crime response

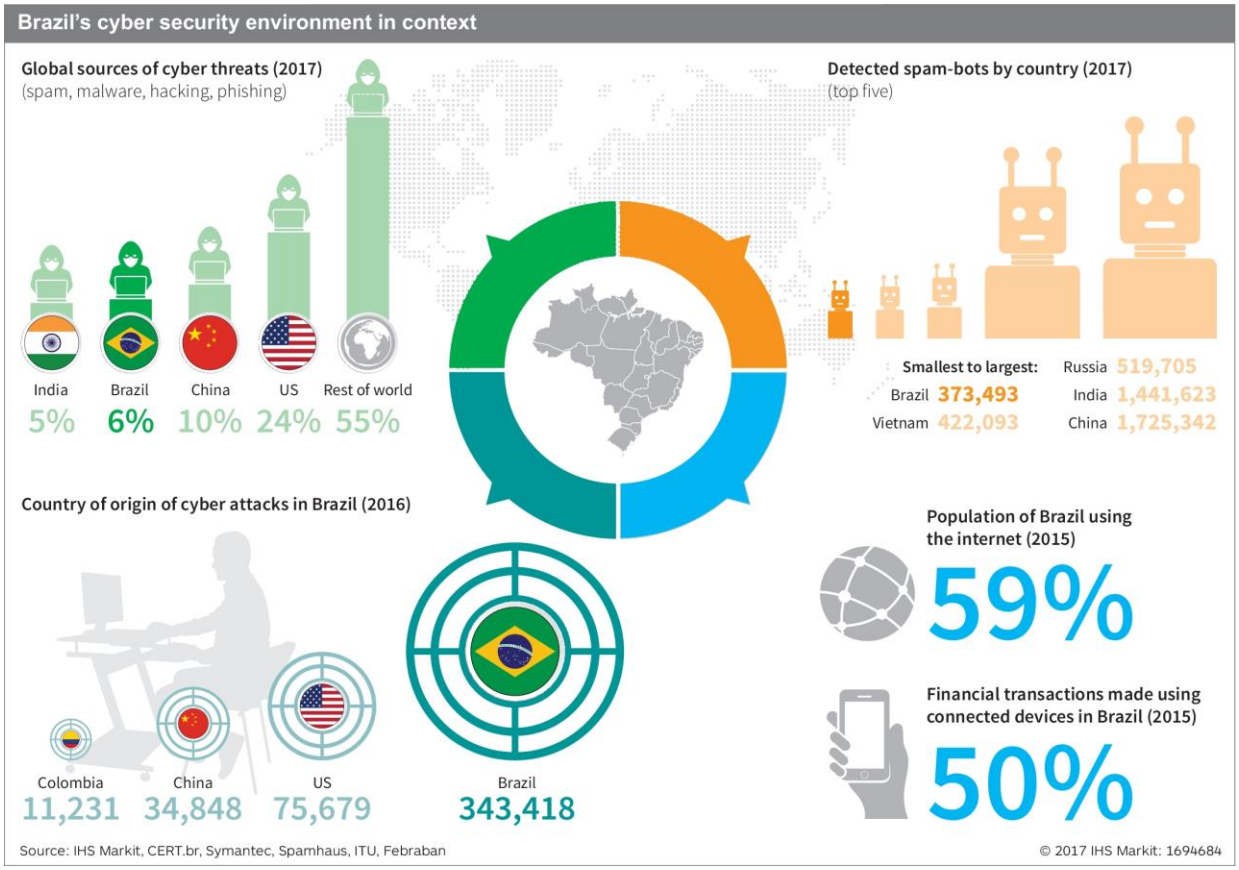
The risk of cyber crime is growing in Brazil amid a debate over the balance between security and privacy. *Robert Muggah* and *Nathan B. Thompson* analyse the nature of the threat and consider the response of the state in a climate of significant economic and political uncertainty

Hours before the opening ceremony of the August 2016 Summer Olympics in Rio de Janeiro, the hacktivist collective Anonymous Brasil launched a series of distributed denial of service (DDoS) attacks on Brazil's state and municipal websites. Operating under the hashtag 'OpOlympicHacking', the group claimed to have successfully crashed five websites, including the games' international and domestic websites, the Ministry of Sport's website, the website of Brazil's Olympic Committee, and the government web portal for Rio de Janeiro. Throughout July and August, other websites were temporarily disabled, including Rio de Janeiro's military police department, the Institute of Public Security, and several public utilities. Such attacks were nothing new in Brazil. Anonymous Brasil successfully targeted websites in 2013, including the country's largest media group, Grupo Globo, the Brazilian national intelligence agency (Agência Brasileira de Inteligência: ABIN), and the Ministry of Justice. Nonetheless, the scale and level of co-ordination of the 2016 attacks marked a new high.

Brazil's government agencies, financial institutions, and citizens are also under threat from groups engaged in cyber crime. In October 2016, a few months after the Olympics had ended, hackers successfully accessed and changed the Domain Name System registrations of all 36 of Brazilian bank Banrisul's online domains. They redirected desktop and mobile users to phishing sites, and are likely to have also redirected data from ATM transactions to their own servers, thereby accessing the credit information of unsuspecting users. In May 2017, the global 'WannaCry' ransomware attack disrupted systems at the Brazilian government's social security authority; the headquarters of Vivo, Brazil's largest telecommunications operator; the public prosecutor's office in São Paulo; and the energy company Petrobras.

The prevalence and sophistication of cyber threats in Brazil continues to increase, according to government statistics, affecting casual users, businesses, and government networks alike. The Brazilian government has recognised the seriousness of this threat, and the Brazilian Congress has enacted a raft of cyber-crime and surveillance legislation, including proposed bills, which, if passed, will make it easier for prosecutors and police to access personal data without a judicial order. In the lead-up to the 2016 Olympics, the government launched a cyber-security task force that included ABIN, the armed forces cyber command (Centro de Defesa Cibernética: CDCiber), and the country's Internet Steering Committee (Comitê Gestor da Internet no Brasil: CGI.br).

[Continued in full version…]



Brazil's cyber security environment in context. (IHS Markit)

1694684

Hotspot for cyber crime

Brazil consistently ranks at the top of global cyber-crime rankings, particularly in regard to botnets, banking fraud, and financial malware. In 2014, for example, Brazil was ranked by Kaspersky Lab, a cyber-security company, as number one in the world for banking malware attacks, with nearly 300,000 compromised users. One reason for this is that Brazil was an early adopter of online banking technology, beginning in the 1990s. The country also has a high concentration of ATMs per capita, with 114 machines per 100,000 people according to World Bank data, against an OECD average of 76 per 100,000. During the 2016 Olympics, ATMs, as well as restaurants and shopping venues, were the main targets for credit card skimming, cloning scams, and more sophisticated crime techniques such as radio frequency interception. Brazil also ranked fifth in a 2017 survey by non-governmental organisation Spamhaus of the world's worst botnet-infected countries.

The targets of cyber crime in Brazil are not limited to government agencies and large organisations. Regular citizens, visitors, and small and medium-sized businesses are also frequently targeted. The Brazilian authorities reported more than 100,000 instances of internet-related fraud in 2016, although this is likely to be an undercount. According to the Brazilian Federation of Banks (Federação Brasileira de Bancos: Febraban), more than 50% of all financial transactions in Brazil are made using internet-connected devices, generating significant scope for cyber theft. Brazil is also a major producer and exporter of cyber crime. A recent report by Symantec, a cyber-security company, places Brazil in third place globally in terms of sources of malware, bots, spam, and phishing attacks, with 5.4% of global threat detections originating in the country.

The number of Brazilians using the internet has increased from less than 3% of the population in 2000, to more than 66% in 2016. In line with this, the number of reported cyber attacks has also climbed sharply, from a low of fewer than 10,000 per year when Brazil first began keeping track in 1999, to a peak of more than one million reported attacks in 2014, the year that Brazil hosted the FIFA World Cup. More than half of all reported attacks in 2015 and 2016 originated inside Brazil, followed by attacks from within China and the United States. Computer security incident reports are recorded by Brazil's National Computer Emergency Response Team (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil: CERT.br) and maintained by the Brazilian Network Information Center (NIC.br), the administrative arm of CGI.br. CERT.br tracks reported cyber incidents, which, although important, are only one metric for cyber crime in Brazil. Actual numbers are almost certainly much higher.

[Continued in full version…]

Policy response and co-ordination

Over the past decade, three discrete policy directives have shaped the country's cyber-security posture and strategy. At the start of former president Luiz Inácio Lula da Silva's second term in 2008, the administration issued its National Defence Strategy (Estratégia Nacional de Defesa : END). This defined Brazil's three "decisive sectors for national defence" as space, nuclear, and cyber. In addition to the END, the 2010 Green Book (Livro Verde) on cyber security laid out a number of basic organisational principles and extended some cyber responsibilities to the office of the presidency. However, there was no clear co-ordination on political, strategic, and operational matters. Finally, the 2012 White Paper on future defence priorities fully established CDCiber, the Brazilian army's cyber command, which has guided much of Brazilian cyber policy. CDCiber's first major task was the protection of the network during the 2012 UN Conference on Sustainable Development (Rio+20).

A man wearing a Guy Fawkes mask, used by the Anonymous movement, protests against the eviction of demonstrators from the former Indigenous Museum, next to the Maracanã Stadium, in Rio de Janeiro, Brazil, on 22 March 2013. Anonymous Brasil has been involved with state and municipal website cyber attacks, especially during the 2016 Olympics. (Christophe Simon/AFP/Getty Images)

1704478

One of the principle obstacles to implementing Brazil's cyber security plans is co-ordinating the broad range of ministries and entities that have some purview over information security and cyber issues. These include ABIN, which is linked to the office of the presidency, and the Department of Information and Communication Security (Departamento de Segurança da Informação e Comunicações: DSIC), which published the Livro Verde and is responsible for information security and cyber security for Brazil's federal government. Nested within the DSIC is CTIR.gov, the presidency's Computer Security and Incident Response Team (Centro de Tratamento de Incidentes de Segurança de Redes), which co-ordinates responses to incidents related to networks connected to Brazil's federal government and public administration.

Brazil's Ministry of Defence plays a dominant role in shaping the country's cyber-security posture through CDCiber, which has been heavily involved in co-ordinating cyber security during Brazil's hosting of international events, including the 2014 World Cup and the 2016 Olympic Games. The Ministry of Justice also retains a cyber portfolio, through the Federal Police and its Unit for Combatting Cybercrime (Unidade de Repressão a Crimes Cibernéticos: URCC), which conducts investigations of crimes related to organised cyber crime, including child pornography. Finally, CGI.br often serves as a consultative body on network security, offering technical expertise through NIC.br and CERT.br. No single agency is tasked with overall co-ordination.

Even so, the revelations by former National Security Agency (NSA) contractor Edward Snowden in 2013 dramatically hastened Brazil's efforts to control its cyberspace. When it emerged that the NSA had engaged in industrial espionage against Brazilian companies – as well as the collection of Brazilian citizens' communications and eavesdropping on former president Dilma Rousseff and other senior government officials – the Brazilian authorities immediately took steps to secure and harden the country's network security infrastructure. This included the construction of new trans-Atlantic internet cables, with six planned over the next two years, linking Brazil's fibre-optic network directly to Africa and Europe without needing to route traffic through North American cables.

[Continued in full version…]

Security versus privacy

At the same time as Brazil's cyberspace has come under tighter government and military control, Brazilians have also forcefully advocated for greater digital rights, universal access, and net neutrality. Brazil's Congress, working with public, private, and non-profit actors, developed and passed a landmark digital rights framework, the Marco Civil da Internet (MCI), in 2014. The law was developed over several years as a multi-stakeholder and participatory model of internet governance that provides for net neutrality, freedom of expression, security, and privacy guarantees for Brazilians. The stability and security of the network has been central to the ongoing debate over the MCI's core principles, and the law was developed in response to proposed cyber-crime legislation. Activists working with the governments of Lula and Rousseff formulated the MCI as a framework of rights and responsibilities for government agencies and corporations, as well as for citizens, to better define and adjudicate the cyber-crime penal system.

As a result, security objectives are frequently at odds with the privacy provisions of the legislation and have fuelled an acrimonious debate between the country's security establishment and digital rights advocates. Despite the accomplishments of the MCI, it lacks a strong, well-defined data protection system, something Congress, the private sector, and civil society have negotiated over the past two years to address in a general data protection law. Conversely, attempts to develop stronger cyber-security laws have met with mixed results. Repeated attempts by the congressional opposition to insert provisions into the civil code for police and government access to data without a judicial order are indications that this fight will continue.

Congressional, law enforcement, and judicial responses to cyber threats – perceived and real – have driven legislative initiatives. In May 2016, the Parliamentary Commission on Cybersecurity (Comissão Parlamentar de Inquérito de Crimes Cibernéticos: CPICIBER) proposed a number of bills with the stated goal of bolstering cyber security. One proposal would compel internet service providers (ISPs) to release the names of users and other personal information associated with an IP address without a judicial order. Another would allow for internet services such as Facebook, Twitter, or WhatsApp to be blocked by judicial order. WhatsApp was previously blocked in December 2015, May 2016, and July 2016 when judges sought access to encrypted communications of suspects of criminal investigations, but in each case the judicial decision was overturned as being disproportionate and a potential violation of the MCI.

The CPICIBER proposals have been criticised by digital rights campaigners as overzealous, but several are still being considered in Congress. Additional legislation under consideration seeks to grant the government greater surveillance and censorship powers, such as the creation of an internet registry. Such proposals, which have been condemned by privacy advocates, would require all manufacturers of computers, mobile phones, and other devices with internet access to record users' names and national identity numbers. Another proposal under consideration since 2015 would require ISPs to collect this kind of personal data – information that would also be accessible without judicial order.

At the time the CPICIBER commission report was issued, Brazil was under immense pressure to stage an Olympics free of major security incidents. Fourteen Brazilians were taken into custody by the Federal Police before and during the Olympic Games under Brazil's then newly minted anti-terrorism law. The suspects, most of whom had never met each other in person, were rounded up in an action dubbed Operation Hashtag and accused of plotting online to commit terrorist acts during the Games. It was the first time the terrorism statute had been applied. Eight of the detainees received sentences ranging from five to 15 years. One of the remaining detainees died at the hands of inmates while in custody at the Várzea Grande prison facility in the state of Mato Grosso. Although probably an exceptional case, Operation Hashtag raises important questions about Brazil's statutory definitions of terrorism and future application of the law with respect to online interactions.

[Continued in full version…]

On the web
- UN body considers international cyber norms
- Cyber security at international sporting events

Author
Robert Muggah is a specialist in security and development and is co-founder of the Igarapé Institute in Rio de Janeiro and the SecDev Group in Ottawa. Nathan B. Thompson is a researcher at the Igarapé Institute, specialising in Brazil's internet governance.