British Institute of International and Comparative Law

Responding to Public and Private Cyberattacks: Self-Defence, Countermeasures and Jurisdiction

International Conference "The Challenge of Global Cybersecurity" University of Granada, 16 September 2021

Yarik Kryvoi
Senior Fellow in International Economic Law
y.kryvoi@biicl.org

British Institute of International and Comparative Law

Nature of public and private cyberattacks

	Private cyberattacks	Public cyberattacks	
		Hybrid cyberattacks	**Direct cyberattacks**
Perpetrator	Non-State actors	Non-State and State actors	States
Motivation for the cyberattack	Usually, financially or ideologically motivated. Private cyberattacks often have an ulterior motif (obtain profit, strike fear or send a message).	A mix of financial, ideological, political and possibility for profit motivations.	Mainly politically motivated, to cause damage or gain access to sensitive information.
Targets and severity of impact	Varies from small to severe but usually targets other non-state entities, rather than states.	Varies from small targets to large targets with severe impact.	Highly severe. Public cyberattacks most often target other states but may also be aimed at non-state actors or own citizens. They can undermine critical infrastructure, national security, democratic legitimacy and institutions, or political freedoms.

British Institute of International and Comparative Law

Forms of private and public cyberattacks

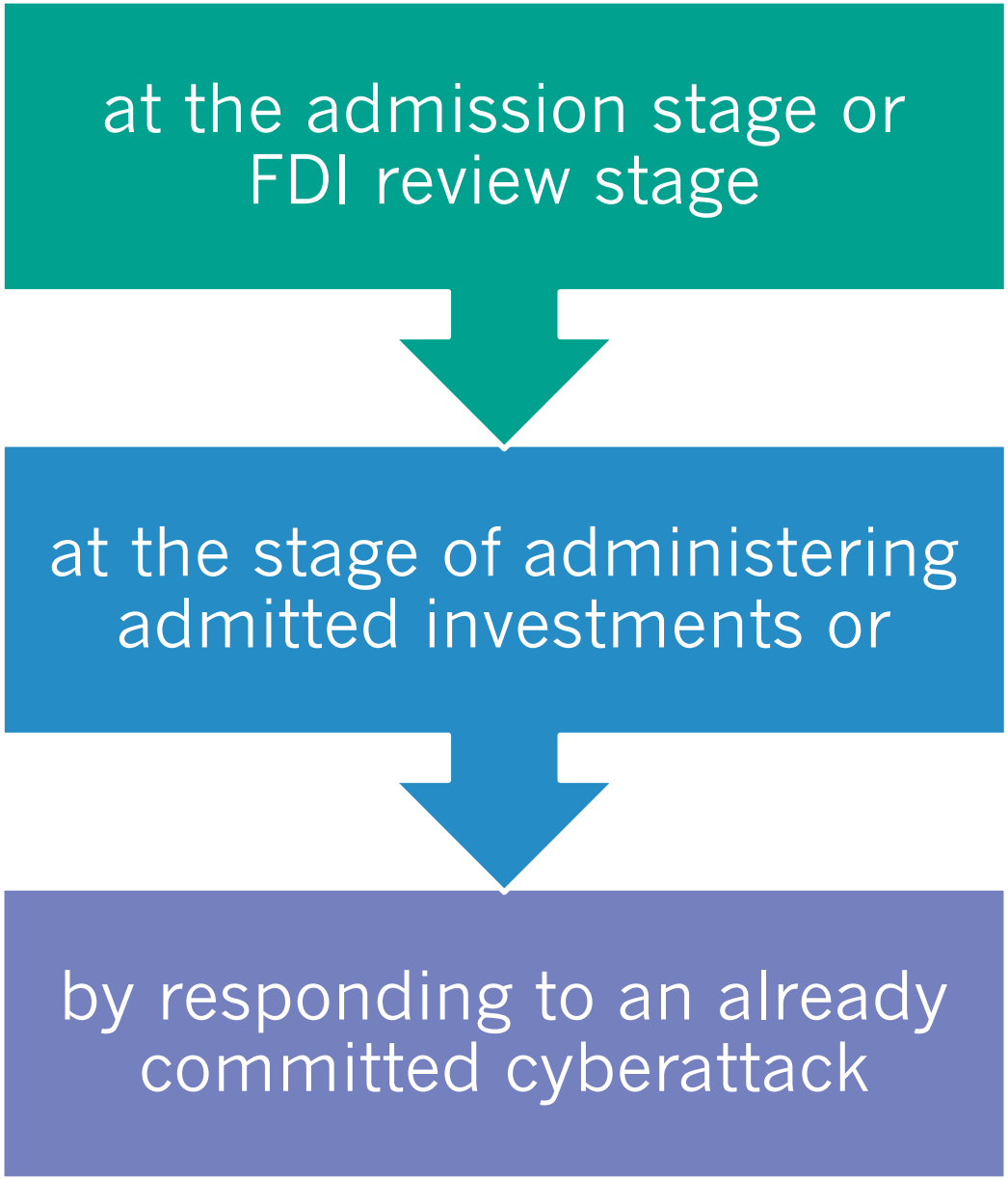
	Private cyberattacks	Public cyberattacks	
		Hybrid cyberattacks	**Direct cyberattacks**
Typical forms	• Ransomware attacks • Personal data leaks • Cyberterrorism • Malware hacking • Child online sexual exploitation • Cyber-enabled crimes	Can take the forms of private and public threats	• Election hacking • Cyberattacks on state digital infrastructure • Attacks on foreign military targets • Cyber espionage • Cyberattacks on the digital freedom of own population

British Institute of International and Comparative Law

Responses to cyberattacks

	Private cyberattacks	Public cyberattacks
Responses	In accordance with domestic laws: - Retaliatory attacks - Confiscation	In accordance with domestic and public international law, including: - Self-defence - Proportionate and necessary countermeasures - Domestic proceedings

Regulators can respond to cyberattacks



Foreign direct investments and cybersecurity

FDI can be a gateway to carry out cyberattacks or engage in other malicious cyberactivity

serve as targets and vulnerable points of entry for cyberattacks

Huawei's 5G network in the United Kingdom

Minimising cybersecurity risks through foreign direct investment screening

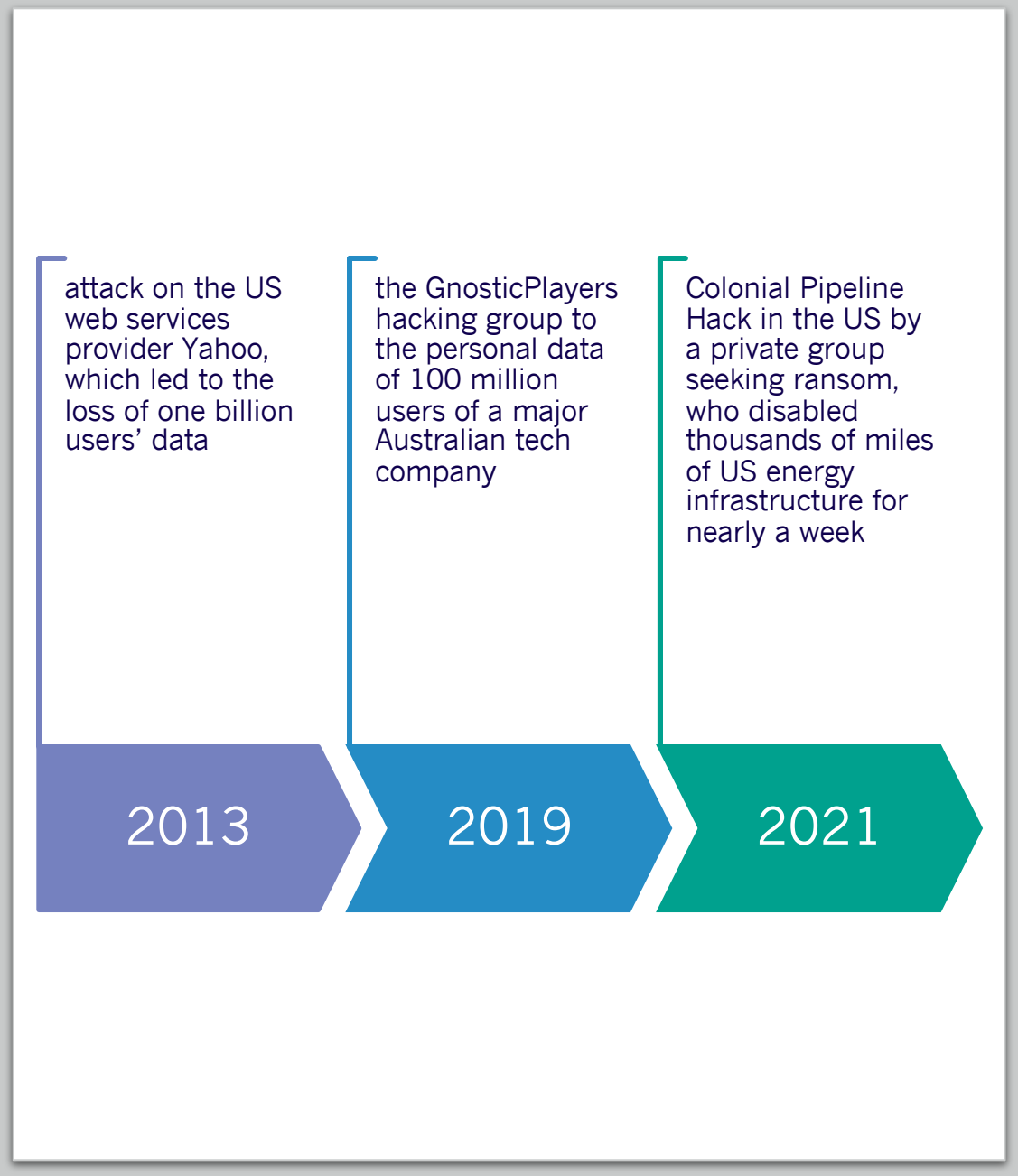
International investment agreements (IIAs) do not address cybersecurity

28 jurisdictions implemented FDI screening procedures, including the EU FDI screening cooperation mechanism

Enterprises that control or access data and cybersecurity at the centre of protecting essential State security interests.

Special monitoring bodies to evaluate potential security threats of foreign investors (e.g., the Huawei Cyber Security Evaluation Centre)

Private cyberattacks



Laws, applicable to private cyberattacks

largely domestic law

2001 Council of Europe Convention on Cybercrime (Budapest Convention), primarily Western states are parties

2009 Agreement on Cooperation in the Field of International Information Security (Yekaterinburg Agreement) by Shanghai Cooperation Organization countries, dominated by China and the US

The Yekaterinburg Agreement mentions the threat of spreading of "information causing harm to political and socio-economic systems, spiritual, moral and cultural sphere of other states" and the domination of the West in the cybersphere

Responses to private cyberattacks

domestic criminal and administrative law measures with possible coordination between states

The US Department of Justice using traditional law enforcement agencies (albeit with new, unprecedented integration of cyberspace strategies) seized the bitcoins used to pay the hackers' ransom

Public cyberattacks

2014 Sony attack by North Korea following the release of the film The Interview

2021 Russian-based hackers, with suspected links to the State, attacked over 150 different government agencies and human rights groups in the United Stated and other countries.

2021 Russian hackers (meaning Russian nationals) conducted ransomware attacks against one of the largest American meat processors. The US government has accused the Russian State of instigating these attacks.

Attribution of cyberattacks to State presents complex factual and legal questions, which eventually determine whether such attack can be regarded as private or public.

Jurisdiction over public cyberattacks

Responses to public cyberattacks are very different from private cyberattacks

bring cases before domestic courts (in 2018, the US charged 13 Russian nationals and three Russian entities with violating U.S. criminal laws in order to interfere with U.S. elections and political processes)

hard to reach States, the ultimate perpetrators, due to sovereign immunity

international courts and tribunals have jurisdiction over State-State disputes

Countermeasures in international law

the UN Charter guarantees the right of States to self-defence against an armed attack

the Nicaragua case highlighted that for self-defence to be triggered, a state usually has to face physical harm but the judgment also suggests that economic harm may suffice as well if it is particularly serious

State responses should evolve using analogies for countering physical force

States may take countermeasures against another State to procure cessation and achieve reparation for the injury, which meet the prerequisite of proportionality and necessity

Examples of countermeasures from domestic jurisdictions

International Strategy for Cyber Space adopted by President Barack Obama (2011): 'certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military partners'

comprehensive sanctions on the Russian economy and specific Russian nationals involved in the hybrid attacks and disinformation campaign

following the 2014 Sony Hack, North Korea reportedly had its internet infrastructure disabled and lost access to the internet for some time.

the 2018 US Department of Defence Defend Forward strategy, the US 'will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict

The back-and-forth between Iran and the United States and its allies over the Iranian nuclear enrichment program underscores the need for a comprehensive re-evaluation of the public international law on cyberattacks to prevent a cycle of unchecked aggression and escalation.

Conclusion

- the importance of the distinction between private and public cyberattacks and different (although overlapping) legal regimes, which apply
- the effective application of existing international law to cyberattacks may require the reassessment of application of the concepts of self-defence and countermeasures in cyberspace
- limited prospects of a global cybersecurity treaty, but close cooperation with allies is possible
- further development of State practice and *opinio iuris* to have more uniform approaches and crystallisation of principles of international law needed