benchtv
a benchmark production

Précis Paper

The Regulation of Australia's Response to State-Sponsored Cyber Attacks

A discussion of the implications of a cyber-attack on Australian soil and the international laws that govern and regulate Australia's response to such an attack.

Discussion Includes

- **Australia's critical structures**
- **Definition of cyber attack**
- **Identification and attribution**
- **International Laws in the event of a cyber attack**
- **When is a cyber-attack an armed attack?**

Précis Paper

The Regulation of Australia's Response to State-Sponsored Cyber Attacks

1. **In this edition of BenchTV, Uche Okereke-Fisher (Barrister – State Chambers, Sydney) and Brett Young (Barrister – State Chambers, Sydney) discuss the implications of a cyber-attack on Australian soil and the international laws that govern and regulate Australia's response to such an attack.**

Australia's critical structures

2. **To date, Australia has never really been a victim of a state sponsored cyber-attack.**
3. **Whilst Australian interests and Australian citizens are routinely targeted for compromise, no state actor or individual actor has sought to undermine Australia's network systems or destabilise Australia's financial institutions.**
4. **The Australian Cyber Centre predicts that in the event of such an attack, the likely targets will include defence facilities and financial institutions, which they consider to be Australia's critical structures.**
5. **Australia's critical structures include physical facilities, supply chains, information technology and communication networks which, if they are destroyed or damaged for an extended period of time, will significantly impact the economic and social wellbeing of the nation, as well as undermine Australia's ability to conduct defence and ensure national security.**

Definition of cyber attack

6. **There is a lack of consensus amongst legal scholars as to terms such as 'cyber-attack', 'cyber war' and 'cyber warfare'.**
7. **However, in general those terms are used to describe conduct or activity that undermine or compromise the functionality of a computer network system for malicious purposes.**
8. **The United Nations International Group of Experts on Cyber Security agree that not every cyber incident will constitute a cyber-attack.**
9. **The Australian Government defines a cyber-attack as a deliberate act to cyber space which manipulates, disrupts, denies, degrades or destroys computer networks or the information resident of those networks for the purpose of undermining national security or de-stabilising the economic stability of the nation.**
10. **This definition looks at the nature of the incident and also the way the incident effects the functionality of the targeted computer system as well as the consequence of the incident in question.**

11. **Another definition of cyber-attack is that prepared by the United Nations Group of Expats who say that a cyber-attack is a cyber operation, whether it is defensive or offensive, that is reasonably expected to cause injury or harm to persons or cause destruction or damage to objects.**
12. **This definition differs from that adopted by the Australian Government by focusing mainly on the outcome of the incident.**
13. **This definition states a cyber-attack only occurs if someone is injured or property is damaged or destroyed. It requires an act of violence and consequential damages to flow from the incident.**
14. **This implies in a sense that non-violent operations, irrespective of the effect that it may have on a victim will not constitute a cyber-attack. For example, cyber incidents that cause irritation or inconvenience such as the outage of a critical network system, will not constitute a cyber-attack under that definition.**

<u>Identification and attribution</u>

15. **In the event of an assumed cyber-attack on Australian soil, the Government's first line of inquiry will be the identity of the perpetrators and to ascertain the nature of the weapons that were employed in the attack.**
16. **The Government will also want to know whether the attack was state sponsored and will then likely seek advice as to the legal rules regarding whether an attack can be attributed to the perpetrators.**
17. **Military and computer experts and cyber security specialists can investigate and register findings that revolve around the identity of the perpetrators.**
18. **However, it is imperative that the identity of the perpetrators is ascertained with a reasonable degree of certainty because the Government does not want to put into place a retaliation plan against a wrongly-targeted state.**
19. **Identifying the perpetrators of the attack is often difficult, as the origin of the cyber-attack will usually be disguised and most cyber-attacks are anonymous, easily being disguised by the user by IP spoofs.**
20. **Identifying the perpetrators of a cyber-attack will be predominantly a technical endeavour and will not necessarily raise any legal questions.**
21. **For when an act or operation can be attributed to a perpetrator, the International Law Commissions articles on the responsibility of states for internationally wrongful acts provide guidelines.**
22. **A cyber-attack is a state sponsored attack if it is authorised by a state and it can be attributed to the relevant state.**
23. **Article 1 of the** International Law Commission's *Draft Articles on Responsibility of States for Internationally Wrongful Acts* **notes that the State will be responsible for its internationally wrongful acts.**

24. Article 4 notes the conduct of the organs of the state, be that legislative, judiciary or executive, will be attributed to the state.
25. Article 5 says that conduct of persons exercising governmental authority, whether or not they are part of the organs of the state will be attributable to the state.
26. Article 8 introduces the concept of degree of control which must be exercised by a state before the conduct can be attributed to the state. This was the question before the court in the case of *The Republic of Nicaragua v. The United States of America (*1986) ICJ 1.
27. In that case the question that was before the International Court of Justice was whether the US could be held responsible for the acts and conduct of the Contras for the purposes of holding the US responsible for the breaches of International Humanitarian Laws by the Contras.
28. On the one hand, the ICJ held that the US was responsible for the planning, direction and support that was given to the Contras however it did reject the broader claim that was put forward by Nicaragua which was that the US was responsible for all the conduct.
29. Upon the facts, the Court preferred a broader construction of the term 'degree of control' and emphasised that a general situation of dependency and support alone, does not justify attributing the conduct in question to the state.
30. In *The Prosecutor v Tadic'* (1999) 38 ILM 1518, the Appeals Chamber of the International Criminal Tribunal of the Former Yugoslavia preferred a narrow construction of the term 'degree of control' and stated that under International Law the attribution to the states of acts performed by individual actors simply requires that the state exercise control over the individuals.
31. The challenges of attribution is furthered by the fact that the state sponsors may well use the services of individual actors and the challenge that arises is the ability to prove that in the first place the conduct was authorised by the states. It may also be difficult to prove that the state did provide all the support that was required to facilitate and enable the conduct in question.
32. Another problem that arises is that in most cases the victim state will not readily put forward information that does acknowledge that its critical infrastructures have been undermined and it is unlikely that the victim state will disclose that its national security has been compromised.
33. There is also a problem of causation with respect to a victim state that would look to make a claim against the offending state as they will need to show a causal connection between the cyber-attack itself and the harm or damages that did or would flow from such an attack.

<u>International Laws in the event of a cyber attack</u>

34. Back in 2010 the United Kingdom's Secretary for Security and Counter Terrorism stated that a cyber-attack that took out a power station did constitute an act of war.
35. However, Uche Oreke-Fisher's position is that a cyber-attack qualifies as an armed attack when it triggers the right to self defence which is available in Article 51 of the United Nations Charter and will then constitute an act of war.
36. The nature and scope of Australia's response in any case will be subject to international law.
37. When the first public disclosure of Australia's offensive capability was made in around April 2016, Prime Minister Malcolm Turnbull emphasised Australia's compliance to International Law obligations and further emphasised that the use of such capabilities would be subject to stringent legal oversight.
38. Whatever Australia's response would be to the hypothetical cyber-attack, would be subject to its international law obligations under Article 2, paragraph 4 and Article 51 of the United Nations Charter.
39. Article 2, paragraph 4 of the United Nations Charter prohibits the use of threat or the use of force against the political independence or territorial integrity of a member state. However, there is no definition for what constitutes the use of force or what constitutes a threat within the Charter.
40. Article 51 of the United Nations Charter protects the inherent right to self defence, whether that be collectively or individual in circumstances where a member state has been attacked.
41. Assuming the response team jumps the identification and attribution hurdles and the cyber-attack is successfully attributed to a state, the team would also have to ensure that any cyber operation that is being planned in retaliation does comply with the prohibition in Article 2, paragraph 4 being the prohibition against the threat or use of force, as well as analyse the circumstances to ascertain whether the right to self defence under Article 51 has been enlivened.
42. The International Court of Justice has emphasised that Article 2 and Article 51 applies to the use of force irrespective of the weapons employed.
43. In respect to cyber operations, it is not the instrument that is used to perpetuate the attack that determines whether there has been a use of force, rather it is a consequence of the operation or the consequence of the attack that determines whether there has been a use of force for the purpose of those Articles.
44. There are two exceptions that do apply to the prohibition on the use of force.
45. The first exception arises where the gravity of the cyber-attack is sufficient to enliven the right to self-defence under Article 51.
46. The second exception to the prohibition is in circumstances where the United Nations Security Council authorises the operation in question.
47. It is important to note that the fact that a cyber operation does not involve the use of force does not necessarily mean that the operation is lawful and that is because it may

constitute a violation of sovereignty and it may also constitute a breach on the prohibition on intervention under the United Nations Charter.

<u>When is a cyber-attack an armed attack?</u>

48. **Article 51 introduces the concept of an armed attack and leads to the questions of what constitutes and armed attack.**
49. **The right to self defence is embodied in Article 51 and that right is enlivened if the cyber-attack does constitute an armed attack and whether a cyber-attack does constitute an armed attack will depend upon the scales and the effects of the cyber attack .**
50. **The law is still unclear as to when a cyber-attack can be deemed to be an armed attack .**
51. **In determining whether a cyber-attack constitutes an armed attack there are three leading views 1) the instrument based approach, 2) The target based approach and t3) he effects based approach.**
52. **Under the instrument based approach, whether or not a cyber-attack constitutes an armed attack depends on the instrument used and under this view, a cyber-attack does not occur unless traditional military weapons are used.**
53. **This approach leaves much to be desired as cyber-attacks are able to cause catastrophic harm or have catastrophic effects without necessarily employing traditional military weapons.**
54. **The target based approach qualifies a cyber-attack as an armed attack depending on the nature of the system that is targeted.**
55. **If it is a case where the system that is targeted is considered a critical system for example any system that falls into Australia's definition of critical infrastructure, will fall into that group**
56. **This approach would deem any operation that undermines the functionality of that system to constitute an armed attack**
57. **The effects based approach looks at the magnitude of the effect and the damage that has been caused by the operation.**
58. **The effects based approach classifies a cyber-attack as an armed attack based on the effect of the cyber-attack which can be based on the sheer severity of the harm or on the duration of the incident in question.**
59. **It is important to note the fact that cyber-attacks do not employ the use of traditional military weapons does not mean that they are not armed attacks for the purpose of Article 51 and in accordance with Article 51, Australia as a victim state would have the right to individual or collective self defence if the relevant cyber-attack is deemed to be an armed attack.**
60. **In contemplating retaliatory cyber operations, it is reasonable for Australia to consider whether or not the international community would deem the incident in question to**

qualify Australia as a victim state and whether the operation it is putting in place violates the prohibition on the use of force and whether the attack qualifies as an armed attack for the purpose of enlivening the right to self-defence.

61. In the event of a state sponsored cyber-attack on Australian soil, Australia's response would include diplomatic measures, economic or military measures and it may well include the deployment of Australia's offensive capabilities

62. These would have the effect of denying or destroying the computer networks of an offending state.

BIOGRAPHY

Uche Okereke-Fisher

Barrister – State Chambers - Sydney

Prior to commencing practice at the NSW Bar, Uche was a practicing solicitor and member of the Law Society of New South Wales. At the NSW Bar, Uche runs a general practice. She accepts briefs on a wide spectrum of practice areas. Her core areas of interest include Employment/Industrial Relations, Commercial Law, Contractual Disputes, Laws of Associations, Administrative and Migration Law, Consumer Protection Laws and Restraint of Trade matters. However, Uche accepts direct briefs from corporations and in-house counsels in all areas of the law. Uche has appeared, unled in a wide range of matters in the Supreme Court, Federal Court, Federal Circuit Court, Fair Work Commission and Local Court.

Brett Young

Barrister – State Chambers - Sydney

Brett Young is a barrister specialising in taxation law and commercial law at the NSW Bar and commenced practising as a barrister in 2003. Brett has practised as a tax advisor since 1994. Brett advises and represents taxpayers in all areas of taxation law, including income tax, stamp duty, GST, land tax and other Federal and State revenue laws. Brett acts for a broad range of taxpayers, including multinational corporations, small-to-medium businesses and high net worth individuals.

BIBLIOGRAPHY

Cases

The Republic of Nicaragua v The United States of America (1986) ICJ 1

The Prosecutor v Tadic (International Criminal Tribunal for the Former Yugoslavia (ICTY) Trial Chamber II, case number IT-94-1-T), 7 May 1997)

Treaties

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, November 2001, Supplement No. 10 (A/56/10)

Charter of the United Nations, opened for signature on 26 June 1945 , 1 UNTS XVI (entered into force 31 August 1965), Article 51 [15:54]; [17:19]; [17:24]; [17:26]; [18:07]; [18:52]; [19:08]; [19:15]; [19:17]; [20:05]; [20:49]