The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility

Colonel David Wallace
Lieutenant Colonel Mark Visger

Colonel David A. Wallace and Lieutenant Colonel Mark Visger[1]

The overarching aim of computer security is to reduce or eliminate risks to an organization's computer networks and cyber infrastructure. One increasingly common way cybersecurity professionals are defending their networks is through the use of so-called "honeypots". The term honeypot has come to mean a deception technique to defend computer systems against malicious operations. Generally, it is an information system resource whose value lies in its unauthorized or illicit use by a hacker. In essence, it is a virtual sting operation. Honeypots can also be weaponized. That is, a honeypot includes files that contain malware that, once exfiltrated by intruders, will cause significant damage and disruption to the intruders' computer networks. The legal issues associated with the use of weaponized honeypots under international law are complex, multi-faceted, and unsettled. This article investigates the legality of using weaponized honeypots under the international law of State responsibility. More specifically, the precise issue addressed is whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility? Ultimately, the answer to the question is "it depends" on the facts and circumstances of a given situation. However, as the analysis below shows, a State should proceed with caution before employing them.

I. INTRODUCTION

When most people think of "honeypots," they picture a plump Winnie-the-Pooh adorably getting stuck while trying to get honey out of a jug—a honeypot. In recent years, the term "honeypot" has migrated to the lexicon of cyberspace and operations. In the rapidly evolving realities of

computer security, the term "honeypot" has come to mean:

> [a] deception technique in which a person seeking to defend computer systems against malicious cyber operations uses a physical or virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment, having the intruders waste resources on the decoy environment, gathering counter-intelligence about the intruders' intent, identity, and means and methods of cyber operations. Typically, the honeypot is co-resident with the actual systems the intruder wishes to target. [2]

Honeypots can be multiple resources such as servers, laptops, web-facing applications or other technological ploys established to monitor and record the actions of cyber intruders. [3] Honeypots are deployed in various ways to make them attractive for hackers. In some cases, they appear to be the "crown jewels" of an organization such as intellectual property, operational plans or financial reports. Intuitively, to be effective, the honeypot must appear realistic. If it looks or feels fake in any way, intruders' suspicions will be raised, and the honeypot will not be effective. [4] In essence, it is a virtual sting operation. [5] Honeypots can also be weaponized. That is, a weaponized honeypot includes files that contain malware that, once exfiltrated by intruders, will cause significant damage and disruption to the intruders' own computer networks. [6] The following example illustrates the use of honeypots to protect critical infrastructure.

Suppose multiple international computer intruders have increasingly attempted intrusions into the computer systems of a large urban water management utility in the United States. The pernicious and persistent hackers have compromised the utility's data historian that manages information from the supervisory control and data acquisition infrastructure network. Such computer operations against the city's water infrastructure are more than just an inconvenience or distraction. More specifically, the intruders have created a real and looming threat because they may be in a position, at some point soon, to shut down water pumps, gates, and valves around the city allowing raw sewage to be dumped into the local waterways as well as creating sewage back-ups around the city. [7] Computer security experts hired by the water utility decide to set a trap to catch the hackers red-handed. They establish three different honeypots which are carefully designed so the intruders will think that they have discovered a computer which controls the physical settings on the water system. The honeypots have fake files, icons, and special security monitoring beacons, making it possible to closely track and observe exactly what the hackers are doing and attempting to do in the network systems. [8] Additionally, the honeypots are weaponized. Destructive malware is incorporated into the honeypots and, upon activation, will cause significant damage to an intruder's own cyber infrastructure.

The legal issues associated with the use of weaponized honeypots under international law are complex, multi-faceted, and unsettled. For legal advisors, policymakers, and academics among others, an outstanding starting point for considering such an important legal

Colonel David Wallace is Professor and Head, Department of Law, United States Military Academy, West Point, New York. In addition to his assignment at West Point, he has also served as a Deputy Staff Judge Advocate; Assistant/Associate Professor at the Judge Advocate General's School of the Army; Trial Attorney, Contract Appeals Division, United States Army Legal Service Agency; Trial Counsel and Legal Assistance Attorney, 3rd Infantry Division; and Public/Civil Affairs Officer, 81st Infantry Brigade. Colonel Wallace teaches a course in the Law of Armed Conflict. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia.

topic as the use of honeypots under international law has already been created, the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* This work analyzes the question of honeypots directly and indirectly as well as many other important topics spanning public international law in its nearly 600 pages of highly informative and influential text. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) invited an independent group of experts to produce the manual.[9] It is important to note that experts were limiting themselves to an objective restatement of the *lex lata* or law as it exists. They scrupulously avoided including statements reflecting the *lex ferenda* or what the law should be.[10] This article investigates the legality of using weaponized honeypots under the international law of State responsibility. Looking at the use of weaponized honeypots under domestic law or in the context of an armed conflict under international humanitarian law is beyond the scope of this article.

II. WEAPONIZED HONEYPOTS: AN ANALYSIS UNDER THE LAW OF STATE RESPONSIBILITY

The precise legal issue addressed in this section is whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility.[11] The law of State or international responsibility, which undeniably extends to cyber activities, "plays a central role in international law, functioning as a general law of wrongs that governs when an international obligation is breached, the consequences that flow from a breach, and who is able to invoke those consequences (and how)."[12] As a threshold matter, under the law of State responsibility, every internationally wrongful act of a State (usually acting through agents of the State) entails the international responsibility of that State.[13] An internationally wrongful act by

Lieutenant Colonel Mark Visger is an Assistant Professor in the Department of Law, United States Military Academy, West Point, New York. In addition to his assignment at West Point, he has also served as Staff Judge Advocate, First Army Division West; Chief, Rule of Law, Multi-National Corps, Iraq; Officer-in Charge, Bamberg Law Center; Government Appellate Counsel; Litigation Attorney, Trial Counsel Assistance Program; Senior Defense Counsel, Fort Rucker, Alabama; Chief, International and Operational Law, Tuzla, Bosnia-Herzegovina; Trial Counsel and Legal Assistance Attorney, 10th Mountain Division (Light Infantry). He is also CompTIA Network+ and Security+ certified. While at West Point, Lieutenant Colonel Visger has taught courses in Cyber Law, National Security Law, International Law and Constitutional and Military Law.

a State occurs when (1) conduct consisting of an action or omission is attributable to the State under international law; and which (2) constitutes a breach of an international obligation of the State.[14] An internationally wrongful act may be a violation of a State's treaty obligations, customary international law, or a general principle of law.[15] Before proceeding with a substantive legal analysis, it is important to note that these rules may seem archaic and ill-suited to the world of cyber-operations. However, customary international law is dependent on State practice. As state practice evolves, a different legal framework for cyber operations may emerge. For now, this analysis reflects the current customary law.

To begin the analysis, one must assess whether the delivery of malware via a honeypot to an attacking State would constitute a breach of an international obligation of the defending State. This analysis would depend upon the effects that the malware creates. If the effects are significant enough, they might be considered a violation of sovereignty, a violation of the rule against non-intervention, or possibly a use of force in violation of the UN Charter. For example, suppose the destructive malware contained in the weaponized honeypot spreads uncontrollably, infecting innocent third parties. If it was reasonably foreseeable that the destructive malware in the weaponized honeypot could and would spread to unintended targets, then the defending State that created and used it bears the responsibility for its internationally wrongful acts. On the other hand, malware that merely identified parties responsible for accessing the honeypot or tracks their activities may not violate international law.

The most likely scenario in the case of malware delivered via a weaponized honey pot would be that the delivery of such malware would violate the

sovereignty of another State, which is considered an internationally wrongful act.[16] The term or concept of sovereignty may be used as a synonym for independence, which is an essential element in being a State.[17] In the often-cited *Island of Palmas* arbitral award decision, the court defined sovereignty as "[i]ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[18] The principle of sovereignty is widely considered to be a primary rule of customary international law, which imposes an obligation on States to respect the inviolability of other States territories.[19] Most assuredly, the principle of sovereignty would encompass cyber infrastructure located in a State's territory.[20] The exact legal character of remote cyber operations by one State on another State's territory is unsettled in international law. However, if physical damage or loss of functionality results from such a remote cyber operation, it would be likely be considered a breach of sovereignty and thus an internationally wrongful act.[21]

If the delivery of the malware through a honeypot constitutes an internationally wrongful act, the responsible State must either provide a legal justification for its acts or it will be responsible under the rules for State responsibility.[22] If there is no legal justification, the State responsible for the internationally wrongful act is under an obligation to cease that act and offer appropriate assurance and guarantees of non-repetition.[23] Additionally, the State responsible for the internationally wrongful act must make full reparations to the injured State.

Possible Legal Defences for Perpetrators of Weaponized Honeypot.

Assuming the malware was significant enough to constitute an internationally wrongful act, the State utilizing a weaponized honeypot may be able to defend the legality of its actions on several grounds. This article will examine each ground in descending order of plausibility.

1. The first possibility is that the defending State did not commit an affirmative act at all, the delivery of the malware was accomplished by the intruding State accessing the honeypot and downloading the infected files. This possibility is addressed by *Tallinn 2.0*, and a majority of the experts concurred with this approach.[25] They contended that the State that accessed the honeypot and then exfiltrated the destructive malware contained within the stolen files is responsible for the damage it brought on itself. More specifically, the defending State that laid the trap did not conduct the actual activity causing the harm.[26] This view does not necessarily lead to the commission of an internationally wrongful act by anyone. The minority, on the other hand, believed that the defending State that placed the destructive malware files in honeypots set everything in motion which culminated, as anticipated, in the damage to the other State's computer system(s)[27] These experts opined that such an operation, at a minimum, violates the sovereignty of the targeted State thus committing an internationally wrongful act, assuming a severe-enough

effect from the malware. Note that this logic would not apply to a situation where malware is transmitted automatically upon access to the honeypot site and which did not require the affirmative step of transmitting purloined files.

The fact that the experts are divided in their analysis highlights the complexities of this issue and the complexities of applying extant international law to this subject. Viscerally, the majority's position rings true and is quite appealing. Namely, it is the intruding State that engaged in a remote cyber operation into the computer networks of the defending State. Moreover, is it not reasonable for a State defending its cyber infrastructure to take measures, like using honeypots, to protect itself against such intrusions and, quite frankly, deter others? Is it wrong for a State to use a dynamic, penalty-based form of deterrence? The law, as it is currently structured, does not address these questions.

2. The next possible justification would be that malware delivered via a honeypot would constitute a valid countermeasure. Countermeasures involve acts that would otherwise be unlawful but are executed as a self-help remedy intended to respond to an unlawful act.[28] The purpose of countermeasures under the law of State responsibility is to cause the breaching State to cease its unlawful actions or omissions, not to retaliate for the previous violation.[29] This is, quite literally, a situation where two wrongs are intended to make a right. Not surprisingly, there are limitations on the use of countermeasures, and a State seeking to use this legal doctrine must craft its weaponized honeypot accordingly.

Before the State operating the weaponized honeypot can claim that their actions are justified countermeasures, it is necessary to consider whether an intruding State committed an internationally wrongful act by engaging in a remote cyber operation in the first place. The answer is, not necessarily. For example, suppose an intruding State is engaging in cyber espionage. Cyber espionage refers to acts undertaken clandestinely or under false pretences that use cyber capabilities to gather or attempt to gather information.[30] Cyber espionage by States does not *per se* violate customary international law.[31] However, the method by which it is carried out *may* constitute a violation of international law such as a violation of the principles of sovereignty or non-intervention.[32] Under this scenario, the method used by the intruding State to engage in mere cyber espionage very well might not violate international law, and thus countermeasures would not be justified.

Another significant limitation to utilizing countermeasures is that they can only be used in response to State-sponsored cyber operations that are attributable to a State under the rules of State responsibility. As a result, a private individual or hacktivist group, operating independent of a State, cannot be subject to countermeasures.[33] The purpose of international law is to govern State-to-State interactions, and the international law doctrine of countermeasures would not apply to non-state actors. This doctrine has one small exception, as States are under a duty of due diligence to prevent cyber-infrastructure within their sovereign control from being used to violate the sovereignty of another state.[34] If the State from which the attack is emanating fails to exercise due diligence,

then the State utilizing a weaponized honeypot might be able to argue that countermeasures against the individuals responsible for the attack are justified.

Assuming that one can establish that the intruding State violated international law during its cyber intrusion, a weaponized countermeasure might be valid, although there are additional requirements to consider. In such a situation, it would be necessary to delve further into the legal requirements of countermeasures to assess whether a weaponized honeypot could be justified as a countermeasure. A State utilizing a weaponized honeypot would have to show that: (1) the damage or destruction caused by the weaponized files is commensurate with the initial internationally wrongful act; (2) that the purpose of the countermeasures is to induce the intruding State to comply with its obligations; (3) that the countermeasures do not affect other obligations such as the protection of fundamental human rights and universal norms; and (4) the State engaging in countermeasures must place the offending State on notice that it is doing so and offer to negotiate.[35] It would likely be challenging to comply with this last procedural condition of notice and an opportunity to negotiate. Suppose the defending State posted an information banner for its networks warning any users or intruders of the possible use of weaponized honeypots. Would that meet the notice requirement? In sum, subject to the comments above, the use of weaponized honeypots as a potential countermeasure cannot be rejected out of hand, although there are significant hurdles to be crossed before a State could legitimately claim that a weaponized honeypot was a legitimate countermeasure.

This review of the doctrine of countermeasures shows that use of this doctrine is difficult in a situation involving highly automated processes, which would likely be the case. The doctrine requires case-by-case legal analysis and is not conducive to an automatic process that delivers malware when triggered in a honeypot. The best possibility to ensure compliance would be to include the malware within files that are designed to be exfiltrated, and then rely on the argument that the attacking State (or private individual) was responsible for downloading the malware (although utilizing automatic delivery of the malware upon accessing the honeypot would likely be much more effective from the defending State's perspective). Regardless, justifying what would otherwise be an internationally-wrongful act under this legal theory contains many pitfalls and would need to be closely monitored.

3. While the doctrine of countermeasures has substantial legal requirements in execution, the doctrine of necessity is much more flexible but has a much higher threshold before it may be utilized. *Tallinn 2.0* succinctly defines the doctrine as: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[36] By its terms, a State claiming necessity must demonstrate: (1) a grave peril; (2) an imminent peril; (3) to an essential interest; and (4) the action taken is the sole means of safeguarding that vital interest from the grave and imminent peril.

While this threshold might be high, the State acting under a legal basis of necessity faces significantly less procedural obstacles due to the nature of the threat. First, the triggering act does not necessarily have to be an internationally wrongful act.[37] Similarly, third parties and non-state actors may be adversely affected by the action under a necessity justification without consequence.[38] Similarly, attributing the intrusion is not required, all that is required is a showing that the intrusion posed a grave and imminent peril to a vital interest and that the action taken was the sole means of safeguarding that interest.[39] This necessity framework may very well be a State's best legal justification for a weaponized honeypot, assuming the requisite threat has been established.

4. The final possibility for justification for a weaponized honeypot that otherwise violates international law is the State's inherent right to self-defence. Codified in Article 51 of the UN Charter, this provision recognizes that a State has "the inherent right of individual or collective self-defence if an armed attack occurs."[40] *Tallinn 2.0* recognizes that cyber operations might rise to the level of an armed attack.[41] Cyber operations could qualify as an armed attack if its "scale and effects" are comparable to that of an armed attack, Tallinn 2.0 provides a helpful framework to analyze whether such a cyber operation constitutes an armed attack.[42] The right to self-defence would justify weaponized honeypots that might otherwise be themselves considered a use of force in violation of the UN Charter. However, actions taken in self-defence must be limited to those necessary to repel the attack and proportionate to the attack and must cease when the attack is complete.[43] This justification would only apply in extreme situations, and likely not applicable to the typical weaponized honeypot.

III. CONCLUSION

As the analysis above demonstrates, the use of weaponized honeypots raises many challenging and complex legal issues under the law of State responsibility. This was also evident in the fact that the experts who wrote *Tallinn Manual 2.0* were split in their analysis. Ultimately, the answer to the question of whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility is "it depends" on the facts and circumstances of a given situation. However, as the analysis above shows, a State should proceed with caution before employing them.

NOTES

1. Colonel Wallace is the Professor and Head, Department of Law, United States Military Academy. Colonel Wallace teaches a course in the Law of Armed Conflict. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Colonel Wallace would like to thank the NATO CCDCOE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship. Lieutenant Colonel Mark Visger is an Assistant Professor of Law, Department of Law, United States Military Academy. He teaches courses in Cyber Law, International Law, National Security Law, and Constitutional and Military Law. The opinions in this article are those of the author and are not intended to reflect those of the U.S. Army, the United States Military Academy, NATO or the CCDCOE.

2. NATO Cooperative Cyber Defence Centre of Excellence *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Michael N. Schmitt, ed. (Cambridge: Cambridge University Press, 2017), 565. When multiple honeypots are used at the same time to create a virtual environment to deceive an intruder, the term "honeynet" is often used to describe such a design.

3. Tari Schreider, "Honeypots & Cyber Deception," *CISO Series on Today's Critical Issues* (March 2017): 2, https://ciso.eccouncil.org/wp-content/uploads/2017/06/Honeypots-Cyber-Deception.pdf.

4. Edward G. Amoroso, *Cyber security* (Summit, NJ: Silicon Press, 2007), 153.

5. Ibid., 154.

6. NATO, *supra* note 2, 174.

7. Tyson Macaulay, *Critical infrastructure: Understanding its component parts, vulnerabilities, operating risks, and interdependencies* (Boca Raton, FL: CRC, 2009), 295.

8. Tom Simonite, "Honeypots Lure Industrial Hackers Into the Open," *MIT Technology Review* (May 8, 2013), np. https://www.technologyreview.com/s/514216/honeypots-lure-industrial-hackers-into-the-open/. This hypothetical is based, in part, on a research effort done by security researcher Kyle Wilhoit.

9. *Tallinn Manual 2.0* is the second cyber law manual produced at the invitation of NATO CCD COE. The first was published in 2013 and focused on the international law governing cyber warfare.

10. NATO, *supra* note 2, 3.

11. NATO, *supra* note 2, 79-80. The customary international law of State responsibility is largely reflected in the International Law Commission's Articles on State Responsibility. This body of law consist of secondary rules of international law. Primary rules set forth international legal obligations. If primary rules are breached, it results in State responsibility. By contrast, secondary rules provide the general conditions for State responsibility and the consequences that flow from breaching primary rules.

12. Silvia Borelli, "State Responsibility in International Law," *International Law - Oxford Bibliographies* (Oxford: Oxford Press January 4, 2018), DOI: 10.1093/OBO/9780199796953-0031.

13. James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge: Cambridge University Press, 2007), 61.

14. Ibid, Art. 2.

15. NATO, supra note 2, 84.

16. Ibid., 17.

17. Ian Brownlie, *Principles of public international law* (Oxford: Clarendon Press, 1987), 80.

18. NATO, *supra* note 2, 84 citing *Island of Palmas* arbitral award, 838.

19.Michael N. Schmitt & Liis Vihul. "Respect for Sovereignty in Cyberspace." *Texas Law Review,* 95, no. 7 (2017), 1649.

20. NATO, *supra* note 2, 18.

21. Ibid., 20.

22. Ibid., 104.

23. Crawford, *supra* note 13, 196.

24. NATO, Ibid., 201.

NOTES

25. Ibid., 174
26. Ibid.
27. Ibid.
28. Ibid.
29. Ibid., 116.
30. Ibid., 168.
31. Ibid.
32. Ibid., 168-70.
33. Ibid., 113.
34. Ibid., 30.
35. Ibid., 111-134.
36. Ibid., 135.
37. Ibid., 137.
38. Ibid.
39. Ibid., 138.
40. United Nations, *Charter of the United Nations* (1 U.N.T.S. XVI, 1947), Article 51.
41. NATO, *supra* note 2, 339.
42. Ibid., 340-342.
43. Ibid., 348.