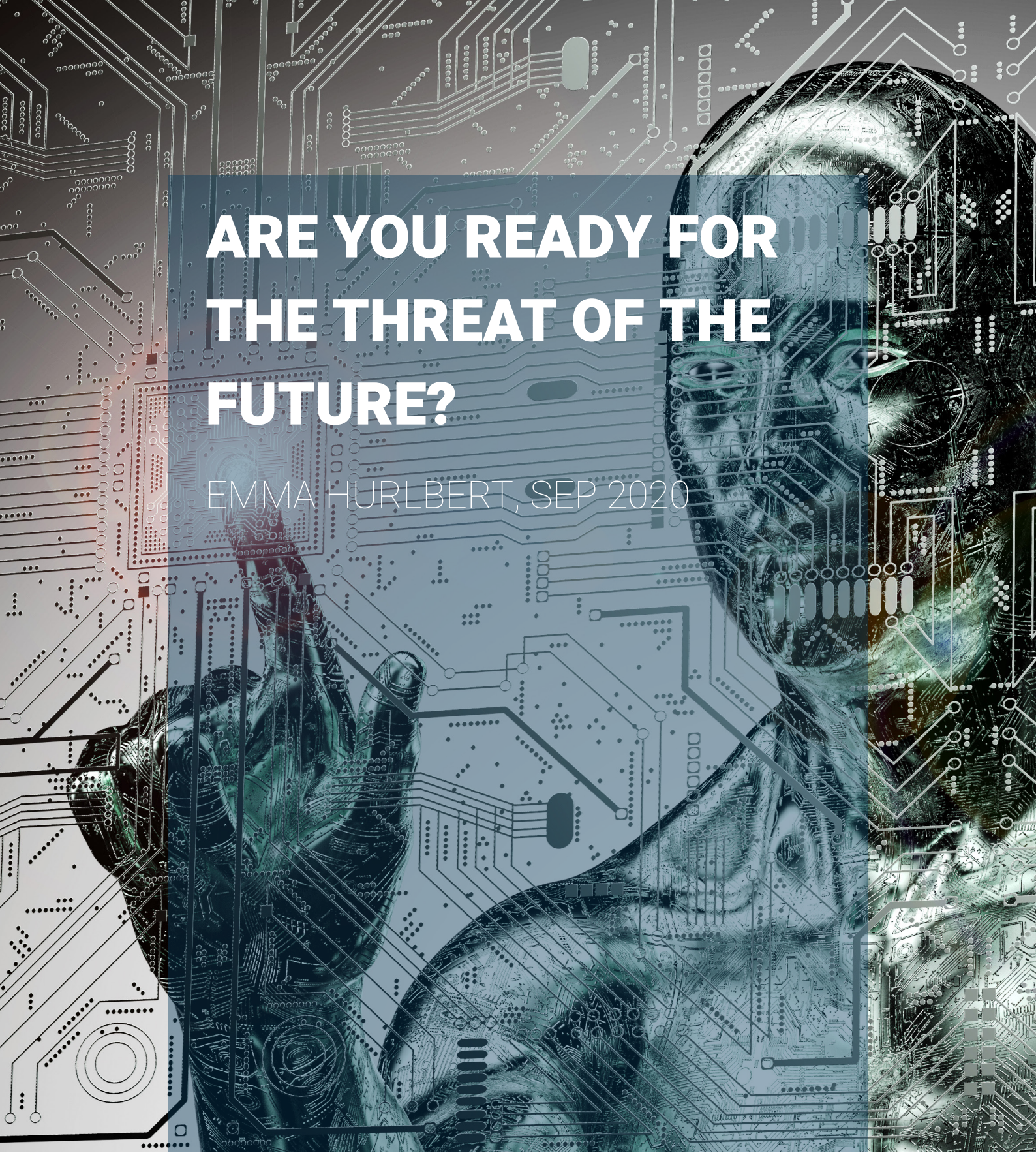

ARE YOU READY FOR THE THREAT OF THE FUTURE?

EMMA HURLBERT, SEP 2020

CONTENTS

ARX

INSIGHT...

The benefits of autonomous ships lie in avoiding collisions and maximizing efficiency, but how can we ensure that our vessels and crew are equipped to complete their journeys safely while assaulted by new threats?

We can also expect to see a surge in cyber attacks through the communication protocol used (be it the internet or other). In this case, the communications between the ship and the shore control centre will open up a new channel for hackers to attack

Traditional pirates often operate similarly to crime syndicates or militias, and it is clear that hacking is not their expertise.

Autonomous ships, greater efficiency, fewer mistakes, changing threats, new challenges to security. The benefits of autonomous ships lie in avoiding collisions and maximizing efficiency, but how can we ensure that our vessels and crew are equipped to complete their journeys safely while assaulted by new threats? Many of us may not need to fully understand the technological workings behind these developments, but we do need to understand the implications of using autonomous ships and how the threats we face will change. This article will provide a brief look at the implications for threats facing autonomous ships at various degrees of their development in comparison to current threats.

These ships, in fact, are not inventions of the far away future, but technologies being implemented currently. The Mayflower Autonomous Ship is scheduled to sail from England to the United States completely autonomously in September 2020(1). These are current technologies, and the industry needs to prepare for how the threats will change as the modus operandi of shipping does.

Firstly, autonomous vessels are not monolithic. There are many different meanings to the term and degrees of autonomy that this term may imply. For the purposes of this paper I use the four degrees of autonomy commonly used in the industry by organisations such as the IMO(2). I note that the four degrees do not necessarily represent a linear and chronological development of autonomous ships; in fact, a lower degree of autonomy may be more likely to become the status quo for the industry rather than the highest degree of autonomy.

ARX

The first degree of autonomy is not a far cry from vessels commonly in operation today, which use automated engine processes such as autopilot and advanced radar systems(3). This degree provides automated services and processes and decision support; the key difference with commonly used ships today being that the automated services in use here would be able to govern themselves to some extent, such as automatic berthing. These technologies will likely see automated process applied where they have not been before: navigation and bridge function management(4). In this case seafarers are on board and can override these processes or step in whenever necessary.

The threats we can expect to see when using technology within the first degree of autonomy would not be extremely different than the threats commonly facing the industry today.

These threats include traditional piracy as perhaps the largest concern, and cyber attacks as a secondary concern. Piracy is combatted by following guidelines laid out in the Best Management Practices 5 document(5), similarly there are recommendations for managing cyber risk, though the last time this was published by the IMO was in 2017(6). Cyber attacks are still considered a secondary concern in this case, because seafarers are on board and can manually negate the effects of an attack.

1

2

The second degree of autonomy will further emphasise the challenges of diverse and complex cyber attacks. This degree of autonomy will see vessels controlled remotely from a shore control centre; however, seafarers will still remain on board in case they need to override or take control. In this case, we can continue to expect the threat of traditional piracy(7), as kidnap and ransom operations will remain profitable for pirates. We can also expect to see a surge in cyber attacks through the communication protocol used (be it the internet or other).

In this case, the communications between the ship and the shore control centre will open up a new channel for hackers to attack, but there will also be seafarers on board that can override communication protocols with the shore centre or manually correct vessel operations and maneuvering.

This degree may face the most risks, as both traditional and emerging threats will be extremely prevalent at this stage and both will be profitable. The industry will need to develop new protocols in order to effectively prevent both types of threats.

3

The third degree of autonomy will see vessels controlled remotely, without seafarers on board. In this case, kidnap and ransom will no longer be an option, but theft of cargo or the vessel itself would continue to be a possible threat to various degrees depending on the defense systems built into the vessel. Widespread utilisation of ships with the third degree of autonomy would create major disruptions in the industry as many seafarers could be laid off. However, the lack of personnel on board would make shipping much safer in human terms, putting less lives at risk on the sea.

This stage may be the most dangerous in terms of cyber attacks and hacking, as there are no personnel on board who could manually override or correct a compromised system.

Since the vessels will be completely remotely controlled, the protocol connecting the vessel to the shore control centre will be a constant target for hacking, without the option for override by seafarers, which may make it the most dangerous stage. This stage will see a lot of changes in how the industry is run and a switch in the biggest threat.

4

The fourth degree of autonomy is complete autonomy: the vessel would operate and make decisions on its own, without the need for remote control. An example of this stage is the Autonomous Mayflower Ship. Once it sets off, this ship will have complete autonomy from land control, making its own decisions for operations based on the conditions it encounters, though it will continue to send information back to the shore centre when connection is possible. Similarly to the previous stage, kidnap and ransom piracy would no longer be an option, though additional protections against theft and capturing would need to be taken. This degree of autonomy would not require as much constant connection to the shore. Therefore, air gaps and closed networks could be utilised internally on the ship to decrease chances of successful hacking.

In this case, hackers would most likely need physical access to the vessel in order to be successful. However, some connection to shore for sending statistics and diagnostics would almost surely still be necessary and open up a possibility for hacking.

In this case, hacking is less likely to be successful, but a successful attack could potentially be more harmful because there are no seafarers nor remote controllers who could override or manually shut off a system. Therefore, once a fully autonomous vessel is hacked, it may have a very low rate of recovery. This stage may see very severe attacks, though with a low degree of success. This stage will witness almost a complete transformation in the main threats facing the industry and preparations should be made now.

ARX

CONCLUSION

As the industry witnesses a change in the main security threats from traditional piracy to cyber attacks and hacking, one must ask, who would be the new attackers? Traditional pirates often operate similarly to crime syndicates or militias, and it is clear that hacking is not their expertise. By assessing the capabilities of current pirates, we can safely assume that a change to hacking would be accompanied by a change in attackers themselves: the industry would face a new adversary.

In order to anticipate where a new threat would come from, we therefore need to look at motivation and capability. Motivation would be found in either disruption and destruction, or profit. As in the famous NotPetya malware attack on Maersk in 2017, it is clear that cyber attacks are not exclusively mounted for profit: they may be motivated by a political statement or disruption(8). As traditional piracy is almost exclusively motivated by profit, this change will complicate the industry's calculations of what motivates attackers. Similarly, the calculation regarding capability is also complicated. Capability will now refer to the ability to both carry out the hacks and to utilize a successful attack for either disruption or profit through selling stolen cargo or a vessel. Needless to say, identifying who will mount complex cyber attacks on various degrees of automated vessels will be a complicated and tedious task, but one which the industry must tackle in order to effectively combat a changing threat landscape.

REFERENCES

(1) "Rethinking the Mayflower: How I Came to Build an Autonomous Ship to Cross the Atlantic," THINK Blog, October 16, 2019, https://www.ibm.com/blogs/think/2019/10/rethinking-the-mayflower/.

(2)"Autonomous Shipping," accessed August 20, 2020, http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx.

(3) Ørnulf Jan Rødseth, "Definitions for Autonomous Merchant Ships," n.d., 22.

(4) Rødseth.

(5) "Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea," Maritime Security Centre, June 2018, https://on-shore.mschoa.org/reference-documents/bmp5/.

(6)"Cyber Security," accessed August 21, 2020, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx.

(7) Security | 14/01/20, "Gulf of Guinea Crew Kidnappings Hit a Record High in 2019 While Piracy Drops Globally," SAFETY4SEA (blog), January 14, 2020, https://safety4sea.com/gulf-of-guinea-crew-kidnappings-hit-a-record-high-in-2019-while-piracy-drops-globally/.

(8) "Maersk: Springing Back from a Catastrophic Cyber-Attack | I-CIO," accessed August 24, 2020, https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

BIBLIOGRAPHY

"Autonomous Shipping." Accessed August 20, 2020. http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx.

Maritime Security Centre. "Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea," June 2018. https://on-shore.mschoa.org/reference-documents/bmp5/.

"Cyber Security." Accessed August 21, 2020. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx.

"Maersk: Springing Back from a Catastrophic Cyber-Attack | I-CIO." Accessed August 24, 2020. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

THINK Blog. "Rethinking the Mayflower: How I Came to Build an Autonomous Ship to Cross the Atlantic," October 16, 2019. https://www.ibm.com/blogs/think/2019/10/rethinking-the-mayflower/.

Rødseth, Ørnulf Jan. "Definitions for Autonomous Merchant Ships," n.d., 22.

Security | 14/01/20. "Gulf of Guinea Crew Kidnappings Hit a Record High in 2019 While Piracy Drops Globally." SAFETY4SEA (blog), January 14, 2020. https://safety4sea.com/gulf-of-guinea-crew-kidnappings-hit-a-record-high-in-2019-while-piracy-drops-globally/.