## THE CONVERGENCE OF MODERN TECHNOLOGY, CYBERCRIME AND MARINE INSURANCE

"Crossing vessel approaching off the port bow" the Second Mate tells the captain as he comes onto the bridge. "We're Stand-On, but she's coming in fast" says the Master. He looks worried. He grabs the VHF:

> *"This is UK registered container vessel MANDSHIP. Calling unidentified vessel approaching my port bow on a heading approx 315°. My course is 045°, speed 16 knots.* ***You are Give - Way vessel****. I repeat:* ***You are Give-Way Vessel****. Please alter course and speed immediately."*

There is no reaction.

The master tries again: *"Vessel now approaching close quarters situation with my vessel. I remain Stand-on Vessel. You are Give-Way vessel.* ***Please alter course and speed immediately to avoid collision****"*
Still no reaction whatever.
But now the Master can see the other ship more clearly.

"No-one on her bridge, Cap'n" says the Second Officer. "Aye, and none on deck either. Looks like the *Mary Deare* - not a soul in sight. Maybe she's one of those drive themselves Google ships - Quartermaster, helm to manual and ready for emergency stations".

… Still the mystery vessel keeps coming ... without course or speed change.

With a collision imminent, the Master tells the Second Mate "No avoiding it now, we'll have to try to turn into her and slip past starboard to her starboard side. It's the only way we're going to avoid a head-on." He then orders hard a-port, full ahead and sounds one long blast on the horn. He reckons that with enough speed he has seaspace to clear inside of the other vessel – which is obviously not going to give way. Responding to the Second's obvious concern, he assures her "The COLREGS allow departures for extreme calls like this one."

But the Master watches in horror as the helm fails to respond: his own ship maintains course and speed. Then a message suddenly flashes up on all the bridge computer screens:

**Safe, Secure Ship? YOU ARE AT OUR MERCY**

**YOUR COMPUTER SYSTEMS HAVE BEEN HACKED AND TAKEN OVER BY OUR OPERATORS. YOU HAVE NO CONTROL OVER WHAT NOW WILL HAPPEN.**
**ONCE THE DAMAGE IS DONE, YOUR SHIP WILL BE PUT IN LIMP MODE TO ENABLE YOU TO REACH A PLACE OF SAFETY.**
**WE WILL CONTACT YOUR OWNERS TO MAKE OUR DEMANDS.**

The Give Way vessel is the AUTOSHIP. The Master was right: she is unmanned. She collides heavily with the MANDSHIP's port side, amidships.

Deafeningly, the two vessels scrape down each other's sides. The anchor in the hawsepipe of the AUTOSHIP gouges deep into the fo'c'sle of the MANDSHIP and rips out part of her bosun's store before the two ships clear.

The mystery vessel continues, speed unabated and course unchanged, until she slows, with systems in limp mode.

The MANDSHIP is badly damaged and requires salvage into a port of refuge, where her owners declare GA. The bosun and an AB require hospitalisation for serious injury. Temporary and then permanent repairs run to many millions of dollars. Her current voyage and two future charterparty fixtures are cancelled, cargo is discharged in the port of refuge, and her entire crew is finally repatriated from the port where permanent repairs are carried out.

The AUTOSHIP is boarded by the Spanish Coast guard and a salvage crew who regain control of her and take her into a safe place in which to tranship her cargo.

***Meanwhile, off the east coast of Scotland ...***

A products tanker is on passage from Peterhead south to Aberdeen. She is fully laden with gasoline. Without warning, the duty officer notices the vessel appears to be veering off her autopilot course – to starboard, in the direction of land. The officer calls the Master to the bridge. "Not sure what's up, Cap" the officer remarks "We seem to be heading off the course you set us for the Aberdeen roads. I'm trying to correct but the helm is becoming increasingly sluggish."

"Steer two points to port" the Master orders. But the helm becomes completely unresponsive and the ship now seems to be heading inexorably for the shore – with a mind of her own.

At that moment, the bridge screens go blank, then show a picture of a Black Hat, followed by the same notice that was flashed onto the screens of the MANDSHIP.

The tanker takes bottom just off Balmedie, on the pristine shoreline of a golf course. There she remains.

Scanning the shore with his binoculars, the Master's blood runs cold when he sees a prominent sign on the edge of the greens....
There is awful pollution, and the golf links has to be closed for a year. (The first letters of demand for consequential losses arrive via Twitter, and the incident spawns a tsunami of #TrumpPollutionLitigation.)

No sooner had the collision and the grounding occurred when a ransom demand flashes worldwide across the screens of viewers of the electronic daily edition of Lloyd's List, warning of further incidents - unless a Sultan's ransom in a selection of cryptocurrencies is paid to the hackers. The ransom notice concludes:

***"We have had a little fun up till now but we will soon start to play our games in earnest. There will be loss of life and massive pollution if our terms are not met within 48 hours. Our tentacles reach wide into your Safe, Secure Shipping industry. We are The Black Hat".***

An insurance investigation team chances upon a link between the three vessels: Although each came from a different yard, all three were fitted with operational and navigational software supplied by Autonav Inc of Boston Ma. Autonav's software technicians installing their systems at the three building yards were infiltrated by sophisticated hackers – the selfsame Black Hat Inc – who left their malware behind.

Further investigation finds that all three ships have similar Doxford main engines with computerised Engine Management Control Systems. All three ships' Engine Management Control Systems had been compromised by Black Hat's infiltrators substituting the regular Intel chips with a lookalike Brightspark chip – which had been preloaded with their malware.

A Marine Court of Enquiry held in London is asked to make a fault finding in relation to the collision. The Court finds that Black Hat's hackers took control of the navigation systems of MANDSHIP, having earlier broken through the ship's firewall protection while two junior officers were playing computer games with their personal laptop plugged into the ship's mainframe internet modem. This was against the vessel's standing instructions. The court accepts evidence from a mole that Black Hat had then taken control of the navigation system of the ship and that they were also able to access the EMCS of the main engine, rendering the ship unresponsive. Their control of MANDHIP was complete.

Evidence shows that the MANDSHIP's firewall protection design was wholly inadequate: the way it had been set up failed to isolate the various computer networks on board. Especially, the network used by the crew for comms was not properly isolated from the ship's operating and navigation systems. This was a flaw in her design.

The Court hears that the unmanned AUTOSHIP was being intermittently monitored by suitably qualified mariners at its control centre in London. No alert was transmitted by the AUTOSHIP to the control centre as it came into close quarters with MANDSHIP. The AUTOSHIP's Autonav software failed to respond and reduce speed and heading appropriately.

Although it is clear that AUTOSHIP's EMCS was similarly compromised, it remains unclear whether Black Hat was able to take control of the vessel before the collision, or whether their embedded malware simply overrode AUTOSHIP's collision avoidance software at the crucial time. It is also unclear whether Black Hat had infiltrated the London Control Centre – although the Centre's software was installed by Autonav. Design security safeguards are called into question.

The Court calls for expert evidence to be heard to determine whether the AUTOSHIP's Autonav on-board software and/or its London control system's software was adversely affected by the known cyber-interference and if so, to what extent. The investigators are tasked also with ascertaining how

the hackers gained control of not only the tanker's EMCS, but also of her ECDIS and navigation systems.

All three vessels are insured on the London Market, with P&I split between London and New York.

**The actions on all three vessels were clearly concerted, connected and meticulously planned.**

*Examine the legal and insurance implications, considering inter alia:*

1. COLREG and SOLAS implications of the collision
2. Seaworthiness implications in relation to all three ships - from a Carriage of Goods and a Marine Insurance perspective
3. Kidnap & Ransom insurance implications
4. Oil pollution liabilities and IOPC Fund exposure in relation to the tanker spill
5. Liabilities for other vessel collision damage, and cross liabilities of vessels, if any
6. P&I implications of crew injury, cargo damage, delay and charterparty cancellation
7. Limitation of Liability implications
8. Cybersecurity on shore and on board all three ships
9. Exposure of the Classification Societies of each vessel in failing to satisfy themselves that the vessels had been in all respects (including electronic systems protection) fit for purpose
10. Product liability for software – including failure of firewall protection and inadequate protection against malware infiltration
11. Liability exposure of the three shipyards and of the software installers.

---

Autonomous ship image: © Techhive.com
Collision damage: Long Kim, taken by surprise, mid Indian Ocean October 1986. Photo by John Hare
Trump International Golf Link photo from www.skygolfblog.com