Game Changers and No Brainers
Ireland's opportunity to lead the world on cyber

by Rois Ni Thuama

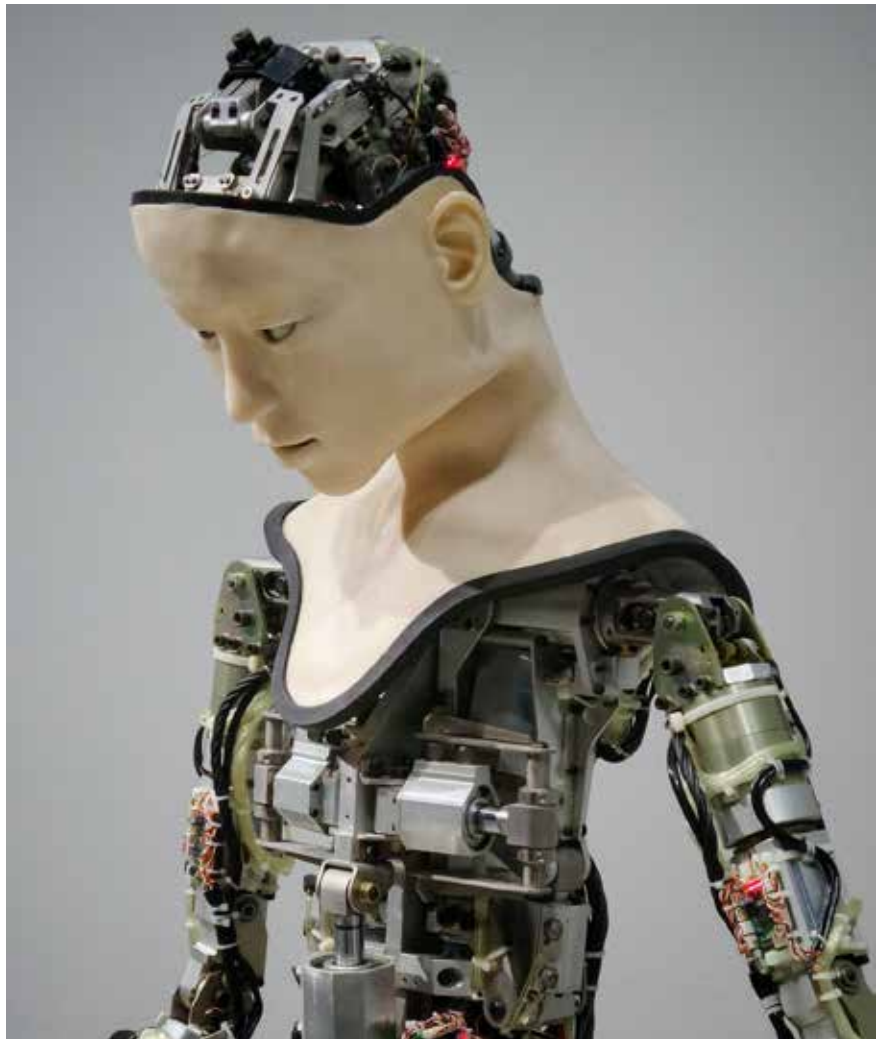
I submit that there exists a perfect storm of elements that when combined could change the Irish cyber landscape with Ireland positioning itself as the preeminent cyber security centre in the world. It will require a combination of adopting new technology, implementing cyber governance best practice and then seizing the moment. Let's start with the new technology.

Anyone who has had the good fortune to have a sneak preview of the capabilities of the GPT-3 (artificial intelligence text generator) is left in little doubt that we are at the threshold of mankind's most exciting development since NASA landed a crewed mission on the moon. To say that GPT-3 is out of this world might actually be helpful. The closest thing I can think of to convey the intelligence that GPT-3 is capable of is to ask the reader to recall the computer on board the Star Trek Enterprise. Communicating with that computer did not require coding. Commands, you might remember could be issued in ordinary language. This is the keystone of this new technology designed by OpenAI.

This feature will make it easier to use and that means that designing and developing new applications will happen faster. It broadens the scope for development because it is no longer confined to programmers. The error rate (bugs) will drop because the code is not susceptible to errors introduced by tired, over caffeinated, overworked eyes.

Anyone who can identify a problem and solution and can articulate that problem / solution in ordinary language can now create and design a new app. This is its inherent genius. How do I know all this?

Rahul Powar, my CEO at Red Sift was one of the few permitted to test drive GPT-3 during its beta phase. As the tech brain behind the Shazam app and Dynamic SPF, as well as the fastest growing cyber security firm in Europe, of course he was.



After a week of comms silence, he showcased its capabilities to the business. For any social scientists that are interested, the sound of nerd euphoria is stone cold silence. The team sat transfixed. Minds boggled with the limitless possibilities. Some applications of this tech were immediately obvious.

For example, one practical application of GPT-3 for accountants would be to assist in crunching large data sets when doing a forensic analysis of spending to identify irregularities.

Instead of needing to eyeball each line of expenses from multiple subjects

across large multinationals, the accountant needs simply to run a list of commands: look at the credit card statements and identify any spending on a weekend or when the person was on leave.

A simple command, such as: review data and find examples of expenses that do not meet the following criteria: travel, accommodation, food and beverage. Then, highlight those examples.

As the AI can be trained, the examples that it found will either serve to reinforce the data subset that it pulled or it can learn that it has not met the criteria in certain instances and hone its understanding. So, if the above command creates odd results, the command could be refined. Alternatively, you can create an example of something that demonstrates what it is you are looking for and have the AI fill in the table. Either of these tactics will improve its results.

Lawyers should be equally excited by this new development. GPT-3 will allow them to investigate and uncover material information in large data sets quickly. Sometimes to obfuscate wrongdoing a subject under investigation might provide more material than was strictly necessary. This is especially true in complex cross border fraud cases. GPT-3 could cut through large blocks of text and unpick the material information through a series of questions.

In some ways it's like sitting down with the most informed person on a subject and then interrogating them. You do need to be prepared to ask the right questions. It's not so smart that it will turn information over like a troubled whistleblower. Human curiosity, ethics and drive are still required to get the best from this new technology.

I asked Rahul, a serial entrepreneur with a talent for spotting smart tech for his views on GPT-3 and he replied:

It is not an exaggeration to say that GPT-3 is a game changer allowing first movers to take advantage and steal a march on later adopters. Getting a handle on GPT-3 now is the key to progress.

Protecting digital assets

Making progress does indeed sound exciting but whatever ground Ireland or indeed any business makes it will also need to protect those advances. Generating wealth and opportunity is one thing, preserving that by making sure you are not haemorrhaging it via easily exploitable vulnerabilities is another. If the path to progress is GPT-3, what is the path to protection for Ireland?

In order to understand what steps Ireland could take to quickly protect the country, its businesses and its citizens from the most significant cyber threats, I reached out to Global Cyber Alliance (GCA). GCA is a non-profit organisation set up by the City of London Police, the District Attorney's office New York and the Centre for Internet Research.

They create practical, scalable, and free tools to eradicate cyber threats. I spoke with their Executive Director for Europe & Africa, Klara Jordan.

Is the proposition that Ireland is in good shape to become a cyber leader credible?

Yes, absolutely. Ireland can become a leader by adopting and promoting measures that improve resilience of the ecosystem through means that require

a relatively low investment but can help significantly improve the overall cyber hygiene.

You have just mentioned (i) 'low investment' that would (ii) 'significantly improve cyber hygiene'. What are the top 3 recommendations from GCA to the Irish Government that meet this benchmark?

The Irish Government should prioritize their focus on three areas:

1. Strengthen the email security of public administration and private sector entities to increase their resilience against spam, phishing and spoofing by adopting, promoting and mandating adoption of DMARC (Domain Message Authentication Reporting and Conformance).

2. Encourage individuals, businesses and ISPs to focus on protection of DNS by blocking access to malicious sites, significantly limiting/reducing the impact of phishing and malicious attacks, through solutions such as Quad9.

3. Work with stakeholders such as chambers of commerce and small business associations to promote the deployment of cyber hygiene controls and free to use tools such as GCA's cybersecurity toolkit for small businesses.

We went on to discuss DMARC in some detail. DMARC is considered layer 1 protection against Business Email Compromise/phishing which is the most significant cyber threat. It is also the starting point for 90% of targeted cyber attacks.

It is little wonder that DMARC has been mandated by the British & US governments for government departments and their suppliers.

Ireland has an opportunity to go beyond the existing standard practice and recommend that DMARC is universally deployed.

This one small step would:

i. materially reduce the instances of cyber crime, protecting Irish businesses, economy and citizens; and

ii. mean that businesses operating in Ireland would be recognised as being part of the most robust supply chain in the world.

If you had to introduce a firm into your supply chain to provide goods or services, do you introduce a firm that has got a robust cybersecurity posture or an inexcusably weak one? The answer should be obvious.

Why Ireland?

It is indisputable that Ireland is attractive to large overseas businesses, as the Financial Times wrote recently: 'Ireland is … a global hub for hundreds of multinationals attracted by its low 12.5 per cent corporate tax rate and EU market access.'1 Ireland's success in the Apple tax appeal cements that position.

Meanwhile its closest neighbour appears intent to continue its undoing as a global leader. Apart from the unusual decision to overlook state actor interference in their 2016 referendum and in their elections in 2017 and 2019, the United Kingdom (UK) is on a course trajectory for a no-deal Brexit. For the UK Brexit means chaos. For Ireland it signals opportunity. Businesses need certainty and access to markets. Ireland offers that.

It gets worse for the UK. To compound this looming self-inflicted period of economic uncertainty, the British government's dithering on Covid and their dilatory decision making led to a late lockdown. This failure to act promptly resulted in England being severely hit by the Covid crisis.

While their tightening-easing-tightening approach to restrictions could be set to the music of the hokey cokey.

By contrast the Irish Government's early lockdown has benefited the country and the economy.

In addition, their overall handling of the Covid crisis was textbook good risk management, outstripping the UK, in testing, tracing and containing this deadly virus. Countries that have managed this risk well, have kept their workforce healthy, and left them feeling confident in their leadership are in a better position to capitalise on technological developments at this time.

I wondered whether there was more to Ireland's strength than simply the neighbours' struggles. To uncover what that might be I managed to track down and speak with Stephen Rae, co-founder of Atlantic Cyber Security Council and Principal at Kobn Leaders' Advisors, which specialises in the cyber and reputation space.

You have spent considerable time in Israel, with leading cybersecurity firms whose solutions are deeply embedded across a range of sectors throughout the world, what do you think are Ireland's strengths?

"Ireland is perfectly positioned to be a world centre of cybersecurity excellence. Our location as an island, our political neutrality, the fact that more than 30 percent of all Europe's data is held here along with the great range of tech savvy third level colleges and universities make Ireland poised to pivot towards being a cybersecurity powerhouse."

What do you think needs to be done and how quickly?

What is now required are policy changes and leadership from the government, first of all to incentivise schools to identify candidates for cyber courses and have the colleges ramp up the variety of cybersecurity courses they offer.

With the right leadership and incentives, including tax breaks for employers and funding for colleges, we can within five years be global players in the cybersecurity space.

1 Financial Times, Apple wins landmark court battle with EU over €14.3bn of tax payments, Javier Espinoza in Brussels, Arthur Beesley in Dublin, Tim Bradshaw in London and Aime Williams in Washington https://www.ft.com/content/1c38fdc1-c4b3-4835-919d-df51698f18c4

Five years is no time at all, and I agree with Rae's assessment. I am energised and enthusiastic about Ireland's future but that is not to imply there is no work to be done.

This drive to promote Ireland as a significant cyber player needs to be approached with a sense of urgency and energy that is not usually harnessed during peacetime.

I reference well known statistics during our conversation. By 2022, there will be a shortage of 350,000 cyber security professionals in Europe. The figure globally is anywhere from 1.5 million to 3 million.

There's a myriad of interesting roles in cyber security, cyber risk and governance.

I ask Rae what steps would you recommend to prepare Ireland for this future?

We shouldn't underestimate the need to market cybersecurity as a career and that it is almost as important an element as having the right third level courses available.

Teenagers will want to be attracted to a career in cybersecurity and that's where marketing on social media and in the schools will be critical.

Conclusion

At the outset I suggested that there was a perfect storm of elements that could facilitate Ireland's role as a cyber leader but on reflection they could be distilled down to two elements. The first is to accelerate progress by way of GPT-3. This new tech is absolutely of the moment and a clear sign of things to come. Every firm and every country that recognises this development for what it is and seeks to ensure that its people are at the forefront of this technology are bound to win. While progress is important, protection is vital.

These are quick wins to promote Ireland and elevate its position as a leader in cyber governance. Address the known significant cyber threats. Treat them with the seriousness that they deserve, begin by mandating them for government departments and suppliers to the government.

Continue to promote best practice and mandate their implementation for all firms operating out of Ireland. Ultimately Ireland is in a solid position to progress with GPT-3 and if the Irish government has the will it can also protect its businesses and economy with the no-brainer solutions as outlined by GCA. What are we waiting for?

Rois Ni Thuama,

A Doctor of Law and subject matter expert in cyber governance and risk mitigation and Head of Cyber Security governance for Red Sift one of Europe's fastest-growing cybersecurity companies. Working with key clients across a wide market spectrum including legal, finance, banking, and oil & gas and writes and presents on significant cyber threats, trends, and risk treatments.