



ROKE

INNOVATION THOUGHT LEADERSHIP



THE PHYSICAL AND THE DIGITAL

To fully understand the world, we need to bring together the physical and the digital. Only by doing so can we accelerate and expand our ability to make sense of the world, to combat disinformation, and to control the environment. In this paper we explore the challenges, and look at how autonomy, AI and common tasking frameworks all help achieve a unified understanding.

CONTENTS



- 1 INTRODUCTION
- 2 WHAT IS THE OPPORTUNITY?
- 3 WHAT ARE THE CHALLENGES AND THE ENABLERS?
- 4 WHAT IS ROKE DOING TO BRING TOGETHER THE PHYSICAL AND THE DIGITAL?
- 5 CALL TO ACTION



INTRODUCTION



“The most successful people in life are generally those who have the best information.”

BENJAMIN DISRAELI, 1804-1881

(quoted in MOD Joint Concept Note 2/18 Information Advantage)

It is no longer reasonable for any operational system to focus on only the physical world or the digital world. Almost everything today exists simultaneously in the real (physical) and virtual (digital) world. Without integration across the physical and digital domains we create multiple points of weakness. We lack access to data. We lack the ability to co-ordinate activities to shape our response to events. We cannot identify and resolve conflicts in data, increasing vulnerability to misinformation and disinformation. It's like missing a primary sense: if we see but don't hear, or hear but don't see, we miss vital information.

At Roke, our mission is to bring the physical and digital together to solve operational challenges. To do this we build on our decades of experience in communications, sensing, networking, software and analytics.

In this paper we explore why multi-domain integration is critical to operations. How can we respond to a rapidly changing situation with speed, precision and accuracy? We argue that multi-domain integration improves the timeliness of response.

More importantly, it also improves the quality of response. Sensing and correlating across multiple domains improves situational awareness. Effective fusion of data identifies and, in many cases, resolves conflicting information. Operating across domains gives a richer suite of actions that we can take. Better data, delivered faster leads to better decision-making and more effective actions.



WHAT IS THE OPPORTUNITY?



Information superiority originated as a military term, but its general thrust is more broadly relevant. It is the idea that we gain competitive advantage from continuous, adaptive, decisive and resilient use of information

Information superiority is achieved when we:

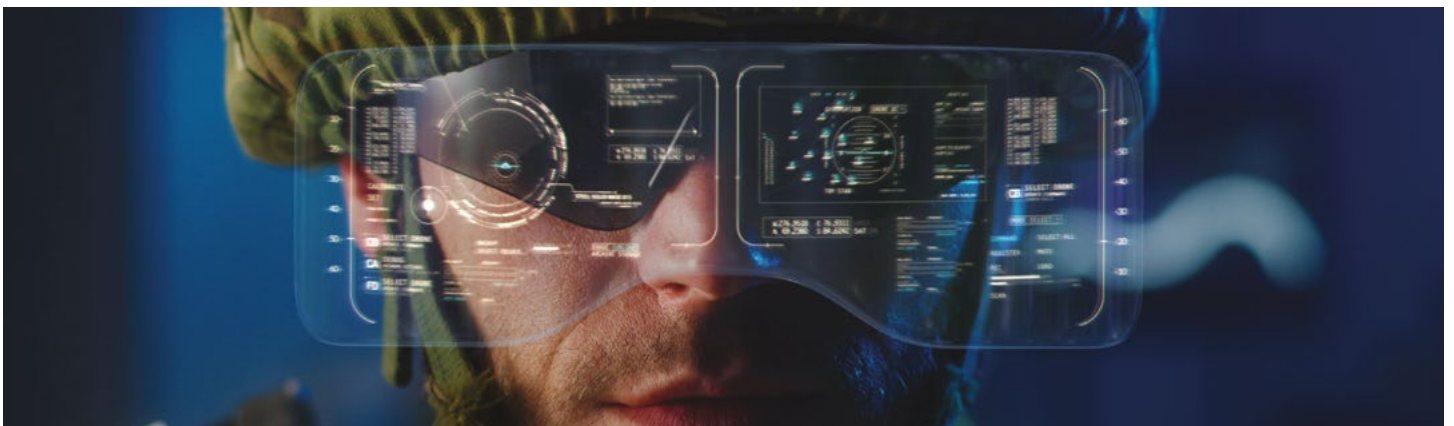
- Build a more accurate understanding of the truth more quickly than competitors.
- Control the information domain, so that we determine an adversary's situational understanding.
- Act proactively and not reactively.

Information can be derived and extracted from a range of sources, both physical and digital. When we walk around, we see and hear what's going on around us. Our brains build and update a picture of the world as we experience it. Technology massively expands our human senses. It lets us see in infrared, pinpoint radio transmissions, use lasers or RF to measure distances. Today, almost all of us also carry a portal to the digital world around with us, sometimes blocking out much of the physical world as we focus on what's on our mobile phone.

With so many sources of data, it would be tempting to take the first and most obvious source – the first picture of the environment; the first article from a web-search.

If we rely on a single source of information, it is easy to be fooled. This isn't new. Soldiers lighting multiple campfires to exaggerate the size of their army has been a tactic since at least the thirteenth century. The allies combined multiple deception techniques to protect the secret of the Normandy landings with Op. Fortitude. This recognised that just using physical deception (like dummy landing craft) would not be sufficient. What has been true through the ages is even more so now.

If we use information sensed from the physical domain and the digital domain and combine it effectively, we can build an accurate picture more quickly.



2

Ships broadcast their location using the Automatic Identification System (AIS); it is easy for a vessel to stop transmitting or send false information. Near real-time satellite data can be used to detect inconsistencies and identify vessels that are trying to misrepresent their position, for example to evade sanctions. We can also use digital technology to interrogate the physical world far more deeply than we could in the past.



We've all seen instances of images being used online to present a false narrative. Sometimes the images are outright fakes or have been edited; sometimes they are shifted in time; sometimes they are from a different location. There are organisations that specialise in detecting this sort of fakery. Much of this can be automated. This will be essential to combat the rise of deepfakes and other deception. Identifying the absence of existing, trusted data may even be a trigger for the collection of new data.



Combining multiple sources within and across domains allows us to effectively detect and even correct false information. Imagine seeing images of a crowd gathering and claims of a riot. We can use visual cues to determine if the content of the image matches the claimed location. With other visual cues and maybe access to public webcams, we can start to see if the information is current and possibly infer intent. If we have access to richer data (e.g. anonymous mobile phone cell statistics), then we can also build a richer picture of crowd density and movements. Privacy preserving techniques can enable information sharing for exploring and resolving conflicts without infringing the privacy of individuals.

If we understand the information domain, then we also know how others will see us. This is obviously useful in a defence, policing, or intelligence environment. Commercial organisations are also very much under attack.

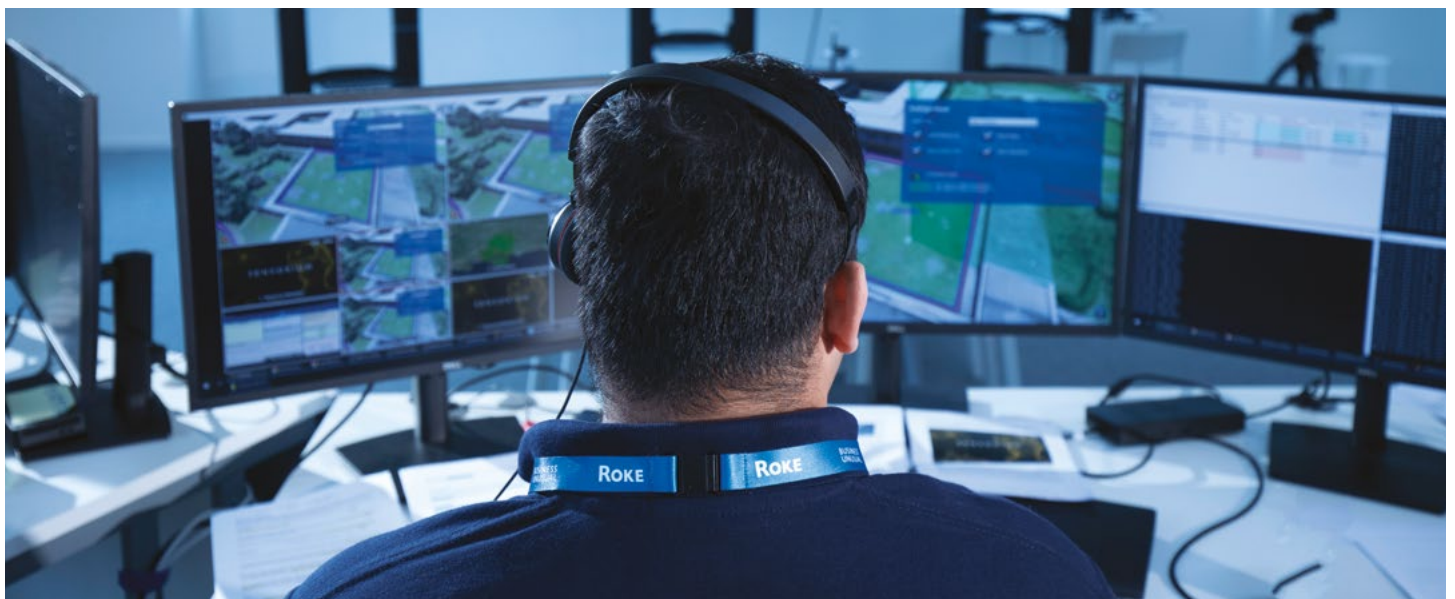
2

Hackers, be they organised crime or state sponsored, are after data, after money or out to cause chaos. The digital footprint of any organisation is being scanned by malicious actors all the time. We need to understand how we appear. What information about the organisation and its employees is available? Controlling the information domain is relevant to everyone.

Not only can the digital domain alter our perception of the physical domain, it can affect it. The Aurora generator test showed how a cyber attack could physically damage components of an electricity grid. Stuxnet is perhaps the canonical example of disrupting physical processes through cyber effect. GNSS spoofing can be used to misdirect ships or drones. These attacks can work through supply chains or by remote access – taking advantage of the global reach of the internet.

As a global entity, it is sometimes assumed that the internet transcends geography. In fact, geography matters a lot. Some countries are known for exerting a lot of control over their digital borders, for example the Iranian internet shutdown. Physical or political control over infrastructure allows not only denial of service but surveillance and other attacks. The US DoD has recently produced a Cyberspace Operations manual that explicitly describes “expeditionary cyberspace operations”. These are operations that require people to be deployed in the physical space to deliver cyber effects. Any facility that relies too heavily on the long-outdated idea of logical perimeter security (a firewall) could be compromised by someone physically plugging in to a network port.

If we understand the physical and the digital domains, we can achieve information superiority.



¹In military terms (e.g. Joint Concept Note 1/20), multi-domain integration refers to all parts of defence working seamlessly together and covers air, cyber and electromagnetic, maritime, land and space. In this paper we use the term to refer to the linking of physical and digital domains, in the absence of a more distinctive term.

3

WHAT ARE THE CHALLENGES AND THE ENABLERS?



The physical and digital worlds don't look or act the same. The physical world is familiar. We see it every day. We consume vast amounts of digital data every day, too, although we don't see how it reaches us. We can interpret other views of the physical world, from infrared cameras, lidar, X-rays, MRI scanners, weather radar or ultrasound: they still relate to the world we live in. The digital world doesn't intrinsically look like anything.

Our challenge is to interpret the digital world, and digital data, in a way that allows us to form a coherent picture of the digital and physical domains. Ultimately, we need to work with both domains and allow information from and about both to be effectively combined and used to make decisions.

That challenge is increased by the volume of data that we need to process. The world is awash with information. From the open internet to the "dark web", free and subscription-based, data is there to be consumed.

```
28 exit_code = 0
29 configure_logging("resolve_wrapper")
30
31 try:
32     config = load_config("../ASNs/Multi/config.json")
33 except FileNotFoundError as error:
34     _logger.error(error)
35     sys.exit(1)
36 except (ValidationError, SchemaError) as error:
37     _logger.error(f"Unable to validate config: {error}")
38     sys.exit(1)
39
40 _logger.warning("Active threads (start): " + str(threading.active_count()))
41
42 multi = None
43 try:
44     multi = MultiSensorManager()
45     multi.setup(config["multi"])
46     multi.select_master("RD03")
47     # setup(address=config["multi"]["RD01"]["address"],
48     # port=config["multi"]["RD01"]["port"])
49 except AssertionError as error:
```

There is no shortage of sensors – from commodity to highly specialised. Those sensors might be fixed or on a mobile platform. From CCTV, a mobile phone carried by a human, a dashcam on a car, a satellite payload, or a sensor on an autonomous vehicle, we have many ways to sense the environment.

Given this endless array of sources, which should we use? Which feed of information will give the most useful information? Do we need all of it? How quickly can that information be gathered? And what is the cost and risk of collecting it?

It's not just the variety and volume of data, but the veracity – or lack of it. The Royal Society's motto is nullius in verba ("take nobody's word for it"). The truth is hard to find. Data fusion, statistical techniques and machine learning are all required, in addition to human analysts, to interpret and resolve conflicting information. Some of that conflict is innocent, arising from noisy, independent measurements. We have good methods for dealing with fusing numerical data. More qualitative nominal and descriptive data is much harder to work with. This will need smarter conflict-resolution techniques, including the use of machine learning. Increasingly, conflict is a matter of disinformation, spoofing or other attempts to mislead.

3

Our approach to collecting and processing data is driven by the need to corroborate and verify our information.

Thinking about having an effect in the world, we face similar questions. The physical world can be affected by direct physical action or by digital activity. Physical actions can also affect the digital domain: jamming can interrupt the flow of digital data or cause communications to be re-routed. Modifications to physical properties can affect the interpretation of information in the digital domain. This could be a deliberate modification, causing autonomous vehicles to misclassify traffic signs or just a system mistake, as where a slogan on a T-shirt was misread as a numberplate.

Having expanded the range of options available to us for sensing and consuming information, planning becomes more challenging. For any given scenario, there will be many assets that could be deployed leading to many different potential plans. How do we select the optimum plan for using the available assets to maximise our knowledge? And not just our knowledge but our trust in that knowledge.

A first, vital, step is to put physical and digital capabilities on an equal footing. When we talk about autonomous systems, what typically comes to mind is a drone or an uncrewed ground vehicle. We describe some of our work with these in our “squads vs swarms” paper. We are also building autonomous digital agents. Those agents can also act autonomously. They can act either independently of an autonomous physical system or in partnership. Importantly, we use the same underlying tasking

approach for both. That enables planning systems to work with and task arbitrary combinations of physical and digital system to meet a goal.

Imagine monitoring the security of a remote facility. With a physical-world mindset, we would go and inspect the fence, the lock on the door, whether the CCTV was switched on. In the purely digital domain, we might carry out a penetration test of any internet-connected network endpoints. When we combine the physical and the digital with a squad of intelligent agents, we can autonomously build a richer picture. Uncrewed autonomous vehicles can inspect the physical environment with cameras and vision processing. We're already using autonomous vehicles with cameras to build accurate three-dimensional digital twins.

The vehicles can exploit other sensors to map out features like wires and survey the RF spectrum. The spectrum survey will reveal active wireless communications endpoints; again, we are already demonstrating this on our low-cost AGV platform. Digital agents, like our reinforcement-learning based AI penetration testing tool, will autonomously explore the site's internet footprint.



3

Others digital agents will use the resources of a ground vehicle and try to scan and exploit discovered wireless access points.

All of the information from this sortie can be collated for centralised analysis, to be presented to a user and used to recommend actions and set follow-on goals.

If we wanted to frustrate someone trying to carry out such an analysis, we would look at how to misrepresent things in both the physical and digital domains. Adversarial patches are images that mean little or nothing to a human but are deliberately constructed to confuse autonomous visual inspection. Dazzling, jamming and other attacks can blind sensors and block command and control. Dummy components and camouflage limit the use of physical inspection. Information seeded into the digital domain creates canaries to alert us to scans. Deepfakes and other misleading information pushed into the digital domain misrepresents the environment and helps control the approach to the facility. Fake access points and even entire virtual deceptive networks lure network and vulnerability scans into wasted operations that present an entirely false picture of the state of the network. All of these false pictures are under our control. We can present deliberately inconsistent information to confuse. We can present different pictures at different times and to different observers.

We immediately see that the information domain is an arms race in its own right. All of these deceptive measures can potentially be detected and countered, leading to yet more sophisticated deceptions and detections.



Our challenge is to introduce autonomy into this process to free the user to work with higher level goals and decision making.

A user will provide high-level tasking in terms of goals and explore the processed, fused and verified findings in both a geographically fixed representation and a logical view. We're continuing to look at ways to improve these visualisations and to find effective ways to help people interact with and query the mixed domains. We are expanding our geospatial views, rendering and overlaying information on three-dimensional reconstructions, and the plotting and exploration of functional and logical maps of data. There are always ways to improve the linkage between views.

Once we free ourselves from the idea that the physical and digital are separable, we open ourselves to a much richer collection of autonomous agents and a much richer view of the world.

WHAT IS ROKE DOING TO BRING TOGETHER THE PHYSICAL AND THE DIGITAL?

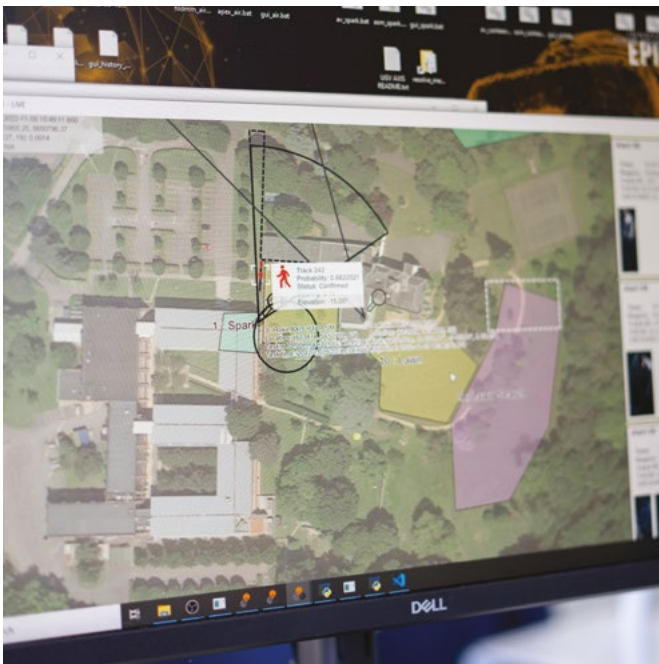
4



We're building autonomous agents, both digital and physical. In the physical domain, we're using our know-how across lots of ways of sensing: cameras, radar, lidar, RF, acoustic. Our digital sensors exploit our knowledge of networks and networking technologies, wired and wireless. Examples of our digital agents include an AI penetration testing tool and Wi-Fi survey agent.

As we build out our command, control and supervision infrastructure², we're integrating both physical and digital agents into a common model. Physical agents can integrate with digital agents, either hosting the agent (providing processing and connectivity) or acting as a communications relay to extend the reach of a digital agent. Our visualisations are designed to be flexible and extensible, so we can use them to represent logical and physical maps.

We are continually developing our understanding, exploiting our ability to experiment with a mixed economy of physical and digital agents.



Some tasks easily extend to a mixed set of agents. Surveying a region, for example, can be done by tasking drones to take pictures and a digital agent to retrieve satellite imagery for comparison. Both are tasked with a geographical region and give back data in the form of images.

Other tasks highlight the differences. Systems that think in terms of geography and range and bearing will not map directly to the internet. Mixed tasking needs to be broken down into specific physical-world and digital-world tasks, even if the agents will be managed via a common interface. There are other differences. Digital agents, like all software, can be replicated at will. We can bring digital agents into being and destroy them in a second. Physical agents can be damaged or run out of power. Both can be detected, but by very different modes of sensing and observation.

As ever, there is no single right answer as to when a physical agent should be preferred over a digital one. Planning needs to take account of the goal, the context in which the agents will operate, and the available set of agents.

²As we move to a more autonomous world, supervision seems like a more appropriate term than control.

CALL TO ACTION




If you've got ideas about working with a mix of physical and digital agents, we'd be interested in working with you. Roke is mature enough to know that we don't have all capabilities and skills within our own organisation. We also recognise the unique position we have in our markets. Roke is committed to ensuring that we nurture an ecosystem of companies that are as specialist and unique as us. We are therefore investing in the resources required to ensure genuine collaboration, thought leadership and problem-solving; bringing together stakeholders with the aim of mutual growth and support of our customers' missions.

Roke's Sensorium is the command and control centre for tasking autonomous agents, analysing collected information, and enabling better decision making. We have a mix of physical and digital agents that we are using to run experiments, exploring how we can use squads of autonomous systems to solve problems. The experiments run in a dedicated space for robotics and using virtual machines and the cloud to provide a digital environment. Tools like our Pattern of Life agents can be used to bring digital spaces to life and generate realistic, human-like behaviour in complex networks.

If you have sensors or agents that would give a novel view of the physical or digital world, we'd like to understand how they could help us. If you have ideas for how to detect and combat misinformation in a multi-domain environment, we'd like to talk to you. We're interested in ideas for experiments that we can run, and understanding how new technology can accelerate our integration of the physical and the digital.





We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK

T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk

© Roke Manor Research Limited 2023 • All rights reserved.

This publication is issued to provide outline information only, which (unless agreed by the company in writing) may not be used, applied or reproduced for any purpose or form part of any order or contract or be regarded as representation relating to the products or services concerned. The company reserves the right to alter without notice the specification, design or conditions of supply of any product or service.