

■ The **Intelligence** Network

Tackling cyber fraud
discussion paper.



Disclaimer: This is an early draft consultation paper and not to be considered final



Disclaimer: This is an early draft consultation paper and not to be considered final

■ The Intelligence Network: Tackling cyber fraud **together**

The Intelligence Network exists to understand, explain and tackle the enduring challenges of cyber security to improve collaboration, simplicity and certainty. Nowhere is this combination more sorely needed than when facing up to the security and societal challenges arising from cyber fraud. Or, nowadays, should that simply be fraud?

Cyber fraud brings together two important challenges faced by society as we adopt new digital technologies: increasing vulnerability of our financial systems to technology-enabled fraud and the increasing prevalence of cyber attacks carried out as a precursor to fraud. To the fraudsters, cyber attacks are simply another step in the process but the way these steps are often spread across multiple individuals, organisations, countries and jurisdictions creates extreme complexity for victims and the authorities.

This discussion paper gathers together initial research and discussions, from what we mean by cyber fraud and why it matters, through to what's standing in the way of reducing or eliminating it. And it concludes by evaluating how we can all work to reduce the prevalence and impact of cyber fraud.

“

We can all work to reduce the **prevalence and impact** of cyber fraud.”

Fraud? Or cyber fraud?

What's the difference between fraud and cyber fraud? Is there one? Fraud is "wrongful or criminal deception intended to result in financial or personal gain"¹. Cyber fraud can be seen simply as fraud that is enabled by technology. Not so much a new type of fraud as a shift in the way fraud is carried out and therefore how it can be detected, investigated and prevented. But 'enabled by technology' struggles to capture the significance of what's changing.

Just as there are myriad ways to commit fraud, there is a broad and ever-expanding range of ways that technology enables fraud. As a starting point, here are some significant traits of cyber fraud:



Remote

Fraudsters and targets are not limited by geography



Industrialised

Able to scale and adopt approaches that were not previously viable



Depersonalised

Using digital identities with limited or no links to real people or businesses



Rapidly Evolving

Techniques can evolve rapidly and build on one another

¹ <https://en.oxforddictionaries.com/definition/fraud>

Why does fraud matter?

Fraud matters because it's so rife right now. Recent crime surveys have found that a person is now more likely to be a victim of fraud than any other crime. Fraud accounts for nearly half of all crimes and over half of all frauds are thought to be cyber-enabled².

Fraud creates or facilitates a wide range of problems. It results in economic losses – both directly and to wider society. It creates a fear of crime. It erodes trust in digital society and business. It prevents law and justice from being administered. And, most chillingly, it enables the financing of terrorism and other criminal activity.

“

Fraud accounts for nearly **half of all crimes** and over half of all frauds are thought to be **cyber-enabled.**”

The impact of fraud on businesses is equally disconcerting. As well as suffering direct losses, organisations are exposed to reputational damage from falling victim to fraud or losing data that puts their customers at increased risk of fraud.

There's confusion around whether cyber fraud is a cyber security or a financial crime problem. Often, it's both. Most cyber attacks are carried out to enable fraud and more than half of all frauds are technology-enabled. To make matters more complex, the individuals or groups carrying out the cyber attacks may not be the same as those perpetrating the frauds, the victims are often different and may be in different industries, countries and jurisdictions. Digital transformation is making it increasingly easy for criminals to exploit this complex interconnected web and society has some catching up to do.

² <https://www.techuk.org/insights/news/item/13518-ons-crime-study-fraud-cyber-crime-still-dominate>



The cyber fraud lifecycle

We normally look at a threat like the actions of cyber criminals through the lens of one organisation. This means we take a narrow view of both the impacts of the attacks and the range of action that we can take to reduce the risk.

	 Cyber Victim	 Fraud Victim	 Financial System	 Law Enforcement
Holds	Valuable data	Financial accounts	Financial intelligence	Legal powers
Suffers	Cyber impact	Fraud loss	Possible liability	Public pressure
Lacks	Direct financial business case	Information Control	Control Legal powers	Information Resources

If we instead look at the end-to-end lifecycle of cyber fraud, the systemic and societal challenges become clearer. At the moment, the system isn't working. Responsibilities and mechanisms that are intended to address fraud are fractured and poorly-aligned to the current problem:

- Criminals mostly need personal information or account credentials to commit fraud. Occasionally this information will be available from public sources but, more usually, some kind of cyber compromise is needed using social engineering and/or technical means. The organisations targeted for this information suffer the technical and possible reputational impact of the compromise but do not generally suffer the direct financial loss of the fraud making it hard to build the business case for greater security.
- Personal information, account credentials or technical access are used to make the fraudulent transaction. This will happen through deception (e.g. Business Email Compromise), coercion (ransomware) or directly using information or credentials obtained, either of the cyber victim or a separate fraud victim. Often, these fraud victims have very little visibility or control over what is happening, especially if they are individual consumers.
- Financial institutions have greater visibility of and control over transactions and they have fraud systems in place which identify and deal with much fraudulent activity. However, where transactions are carried out using legitimate but stolen credentials or relate to subsidiary processing or money laundering, individual financial institutions often do not have the information or powers to block them.
- Money laundering and other compliance reporting regimes provide law enforcement organisations with a source of financial intelligence but these schemes were designed some time ago and tend to provide limited information that law enforcement finds difficult to turn to direct action.

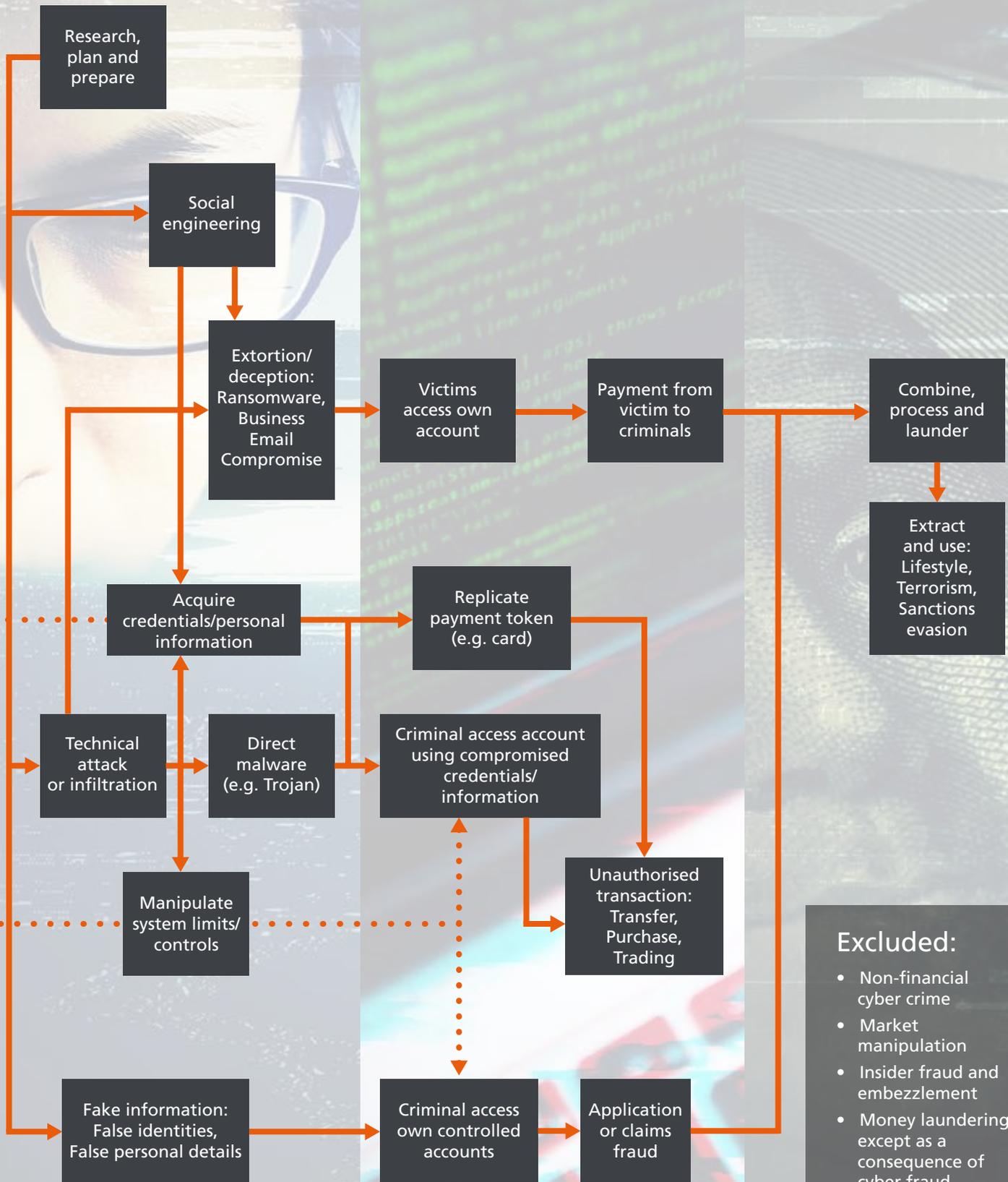
Given these split responsibilities and misaligned incentives, society's action to reduce cyber fraud is fragmented and less effective than it could be. As a result, the opportunity and return on investment for criminals conducting cyber fraud is significant and growing.

A more detailed view of the lifecycle is included in the annex, including the path taken by different types of fraud.

Cyber Attack

Fraudulent Transaction

Process Funds



Excluded:

- Non-financial cyber crime
- Market manipulation
- Insider fraud and embezzlement
- Money laundering except as a consequence of cyber fraud



Cyber Victim



Fraud Victim



Financial System



Law Enforcement

The potential for tackling cyber fraud

While individual participants lack all the pieces necessary to make a substantial difference, taken together society has the information and power to make these crimes more difficult, shift the return on criminal efforts and so reduce the attractiveness and prevalence of cyber fraud.

The challenge is one of co-ordination, co-operation and alignment in a world of thousands of financial institutions and law enforcement agencies and millions of potential cyber and fraud victims. This will not happen quickly or through central planning but it is possible that a substantial difference could be made over the medium term by changing the economics and mechanisms of interactions between the four groups set out above.

The greatest effect is likely to come from more reliable, effective and repeatable organisational cyber security and a reduction in the technical and organisational barriers that currently prevent this and so leave opportunity for the criminals.

Regulations such as the EU's GDPR provide a welcome renewed impetus to the corporate management and protection of personal information but the fear of fines means most organisations are focussing on narrow, local compliance and risk avoidance. As we move beyond initial implementation, there is an opportunity to develop this into a more collaborative and constructive approach that can improve the security of society as a whole.

What's next?

We're going to be taking the ideas we've outlined in this discussion paper to industry bodies, experts, customers, partners and The Intelligence Network to gather feedback on the challenges surrounding cyber fraud. We want to start tackling fraud as a community – making a significant and lasting contribution to a safer digital world.

To add to the conversation, and find out more about The Intelligence Network, visit: boesystems.com/theintelligencenetwork/

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: theintelligencenetwork@baesystems.com | W: baesystems.com/theintelligencenetwork

 [linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)

 twitter.com/baesystems_ai

Copyright © BAE Systems plc 2018. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.