Wilton Park

Report: Enhancing international cooperation on cyber regulation

4 – 6 March 2026

In partnership with the UK Department for Science, Innovation and Technology, with support from techUK.

In partnership with

Department for Science, Innovation & Technology

With support from

techUK

Executive summary

Cybersecurity regulation presents a fragmented landscape. This fragmentation can place a high compliance burden on regulated organisations while not necessarily improving security outcomes because a disproportionate amount of time and security budget is spent on administrative tasks rather than fulfilling critical cybersecurity functions.

The Wilton Park Dialogue showed that there is opportunity for governments and stakeholders to convene in an international effort to improve regulatory coherence across jurisdictions. This report identifies five core themes of the current situation discussed at the Dialogue and ten recommendations that would make a tangible difference for regulatory alignment. Participants discussed which organisations could take on the specific tasks, which included those present at the Dialogue as well as other institutions such as the Organisation for Economic Cooperation and Development (OECD) and the Group of Seven (G7).

1. **Focus on 'why'**. Regulation should be considered only where crucial, and it should be shaped by a clear understanding of its ultimate purpose: maintaining resilience of important digital systems and keeping people safe. Certain good practices should be deployed in regulatory policy development to ensure that regulations fulfil this ultimate purpose, are effective and efficient, and are coherent with approaches in other jurisdictions.
    - **Recommendation I**: Create common 'good practice' principles for developing cyber regulation and ensure these principles are utilised.
    - **Recommendation II**: Develop a decision-making framework for policymakers, to guide the utilisation of these principles and to help signpost users to useful resources (eg, useful existing research and other forms of evidence).
    - **Recommendation III**: Focus on tackling divergence around incident reporting requirements, which should bring immediate benefit to both regulated businesses and regulators. Agreeing on the fundamental purpose of this reporting may help jurisdictions move closer to aligning on the requirements they set.
    - **Recommendation IV**: Consider the role that AI can and can't play in tackling the problem of cyber regulatory divergence across borders.

2 **Political support**. Meaningful international regulatory cooperation on this topic requires high-level political buy-in. This is because cybersecurity is a cross-cutting domain, and choices around cybersecurity regulation can also have important national security, socioeconomic resilience, and economic competitiveness implications.

- **Recommendation V**: Secure buy-in from key players in national cyber regulatory ecosystems as well as a central executive body of government
- **Recommendation VI:** Improve the evidence base around the economic cost of misaligned cyber regulations.

3 **Taxonomy**. There is ample disagreement on definitions of core terminology used in cybersecurity regulation, and "speaking the same language" is a pre-requisite to international regulatory coherence.

- **Recommendation VII**: Create a common taxonomy, building on existing resources.

4 **Trust**. Cooperation on regulation requires trust in two aspects: international trust for coalition-forming, and trust in people doing work and the way that work is done.

- **Recommendation VIII**: Support the creation of a mechanism to provide strategic direction and to support monitoring and accountability for this work.
- **Recommendation IX**: Create an internationally shared cyber assurance model.

5 **Sovereignty**. It is likely that certain regulatory requirements will remain misaligned. This is because national cyber regulations are linked to diverse threat pictures and socioeconomic contexts, and governments have different risk appetites and different levels of concern for digital sovereignty. However, if governments can align on 80% of their requirements, that will make a substantial difference to businesses' compliance burdens.

- **Recommendation X**: Construct and offer a regulatory requirements menu.
- **Recommendations I, II, VII and VIII** also contribute here.

Introduction

Digitisation in organisations, combined with cyber threats emanating from a range of sources, has exposed critical cybersecurity vulnerabilities across countries' economies. Given that the market has not successfully addressed these challenges by itself, many governments have intervened to establish, or are developing, cybersecurity regulations. However, differing approaches in the development of regulations have resulted in regulatory divergence. This divergence, in turn, places additional burdens on regulated organisations that must now comply with regulations across different jurisdictions. Aside from the economic cost of compliance, industry voices have also noted that the weight of adhering to these new requirements may also lead to 'box ticking' rather than thorough efforts to build meaningful cybersecurity. Industry has called for greater coherence in global cybersecurity regulations and for government-led progress in this space.

Fundamentally, there is an opportunity for governments to convene together with stakeholders to formulate 'good practice' principles for developing cyber regulation in a way that should reduce fragmentation. There is a need to expressly recognise that a problem exists, to understand the causes of the current situation, and build a shared commitment to improving it. Within this, stakeholders must be afforded opportunity to share their experiences and points of view. Further, there are both overarching approaches to regulation as well as specific details of cybersecurity which require elucidation. This clarification should help to identify the tangible actions that can be taken to impactfully address: i) issues identified in current regulations; and ii) the development of future regulation.

These efforts will help build an international community of partners who, with different strengths, can collectively achieve greater interoperability and cooperation around cyber regulation.

Focus on 'why'

Regulation does not arise spontaneously; it is the result of careful deliberation by policymakers. Indeed, due to cost implications, regulation is a tool of last resort wielded only by governments when two conditions are met: a market fails to self-correct against (perceived) harms to consumers, the economy, or the environment; all other measures short of regulations, such as incentives, voluntary codes of practice or technical standards, have been exhausted without having the desired effect.

For cybersecurity, there is an opportunity to focus on why governments have decided that regulation is required and what the intended outcome is. Although governments are often driven by similar imperatives, fragmentation is introduced, for instance, when i) regulation is used to pursue too many objectives; ii) when evidence for policy design and review is lacking; or iii) when regulations are developed without reference to existing international standards and norms.

Cyber regulation should be shaped by a clear purpose and designed to introduce only the minimum distortions necessary to achieve that purpose. The purpose should be maintaining resilience of important digital systems and keeping people safe. Focusing on the 'why' of cyber regulation leads to several potential actions.

First (**Recommendation I**), the process by which regulation is developed can be harmonised. At present, even if countries independently arrive at a similar decision that cyber regulation is required, once they reach this point, there is divergence in the way this regulation is developed, which results in different requirements. By adopting common approaches to regulatory development, countries are more likely to translate shared regulatory objectives (the 'why') into aligned regulatory requirements.

There is merit to developing a set of principles that could be used by governments to design and implement cyber regulations. Examples of such principles might include: i) anchoring regulations in international standards; ii) utilising common terms and definitions; iii) striving for co-creation with industry; iv) ensuring that regulations are evidence informed. The approach would benefit from being risk-based and largely or entirely outcomes-based, and should consider special measures for SMEs.

Participants suggested that an organisation like the OECD would be well-placed to develop and promote this work. The OECD is a well-established norm-setter and can convene different communities (for instance, through its regulatory policy work as well as its digital security work), and it could develop these principles as an OECD Recommendation. A major focus of this activity should be ensuring that any principles are adopted and used consistently in regulatory development processes.

Second (**Recommendation II**), a decision-making framework could be developed. This framework should help legislators when they run into questions around how to implement certain principles or where certain principles seem to conflict in a particular setting.

Third (**Recommendation III**), one area of cyber regulation that could be prioritised for more immediate wins is incident reporting. Existing regulations are generally very prescriptive around incident reporting, and detail between jurisdictions differ greatly, for example, around what qualifies as an incident, what information must be contained within a report, and within what timeframe an organisation must report an incident. Relatively small changes to incident reporting requirements could significantly reduce the burden faced by regulated organisations as well as regulators. More developed thinking about the purpose of incident reporting can help clarify timeliness, proportionality and information sharing, which can ultimately improve the interoperability of regulations.

Finally (**Recommendation IV**), the proliferation of artificial intelligence tools warrants consideration of the role AI might play in addressing the problem of fragmented cyber regulation. Part of the problem of fragmented regulation could potentially be addressed through AI, for instance, by handling the administrative burden or duplicative requirements. However, AI is not a silver bullet, since it cannot handle conflicting requirements and it cannot decide what to report. In thinking about the 'why' of this initiative, it is worth unpicking areas that cannot be resolved through AI as a priority.

Political support

While cybersecurity is inherently a technological domain, regulation is a policy matter. Cyber regulation should be grounded in a deep understanding of the technical dimensions of the problem and of different response options, but it will also be informed by political choices. It is also a cross-cutting domain, which is linked to many different public activities and ministerial portfolios.

International cooperation on cyber regulation will require high-level buy-in and active support. This is for a variety of reasons, including: i) it will force trade-offs that only senior leaders can resolve, ii) it will require coordination across powerful institutions; iii) it signals credibility to partners and industry (that the direction of travel is stable); iv) it manages risk and accountability. A senior governmental champion can also help to marshal resources and inspire action. The core recommendation (**Recommendation V**) here is to identify and secure buy-in from a senior public figure who has significant influence in decisions made around cyber regulation, as well as a key figure or figures within a country's executive branch. The former would create a banner under which

other regulatory cooperation activities can be unified, and the latter would support coordination and additional pressure, where required.

Additionally (**Recommendation VI**), a rigorous analysis of the economic cost of misaligned cyber regulations could be developed. Such an analysis would explain to policymakers why they should care about this issue, why they should consider taking reform measures (that may not be easy) to address it, and which intervention areas they should prioritise. It should also help build political support behind reforms. Participants expressed the view that the OECD, which is an established and respected authority for data collection and analysis, would be well-placed to take this work forward.

Finally, they have also agreed that a high-level platform such as the G7 Leaders' or Digital and Technology Track could be used to advocate for international cyber regulation cooperation and to highlight, at a high-level, cooperation in this space. This would help raise awareness of the initiative to participating governments, as well as among industry and other stakeholders in those countries.

Taxonomy

It is abundantly clear that cyber regulation is rife with specialist terminology. This is expected, given it is a technical field, but it becomes a problem when the international community lacks agreed definitions on core terminology. Across jurisdictions, a term may be used to refer to different concepts/requirements, while different terms may be used to describe the same concept. The lack of consistency across the international landscape leads to different cyber regulations. For example, the definition of a reportable 'incident' can vary significantly between countries, even where regulations use the same term: 'incident reporting'. Therefore, regulated entities need to keep track of these different definitions to know whether an incident triggers a reporting requirement in any given jurisdiction.

The recommendation (**Recommendation VII**) that flows from the terminology problem is to create a taxonomy. A taxonomy would contain agreed definitions to create a baseline from which governments can derive cyber regulations. By using the same terms consistently, countries can avoid unintended divergence between their cyber regulations. Participants noted that an institution like the OECD could take this forward, utilising existing resources (for instance, taxonomy work developed by the

European Cyber Security Organisation) and potentially working with other partners, including those that attended this Dialogue.

Trust

Central to regulatory cooperation is trust. Trust is required both at the international level and the operational level. International government-to-government trust is a critical part of forming coalitions, which can be a vehicle for furthering dialogue (under the political banner outlined above) as well as inviting additional countries into the fold, thereby increasing the reach and effect of regulatory cooperation. At an operational level, trust is about the people delivering cybersecurity work, especially assurance work, and the way that work is done. Trust in the (assurance) process results in trust in the outputs of the process; in practical terms, regulators and organisations can use outputs produced by international partners without a high degree of additional scrutiny.

To build these kinds of trust, two recommendations should be considered. First (**Recommendation VIII**), regulatory cooperation requires steering and coordination. To meaningfully address the problem, action will be required in different settings, and it would be helpful to give legislators and regulators a view of what is happening across these different settings. Some kind of coordinating body or instrument should help increase transparency around the actions taken by participating legislators. Additionally, it could be used to share resources, challenges, and to identify new areas where interventions may be needed (for instance, new standards development work, in an area that might be ripe for regulation). This mechanism should also be used to ensure that efforts to address this problem are truly multistakeholder, and that different stakeholders can feed views into fora where they might not have an equal seat at the table.

Second (**Recommendation IX**), directly addressing the opportunity to create trust in assurance work, there is an opportunity to create a shared cyber assurance model. This model would be used by assurance bodies to ensure confidence in the way assurance work is carried out in different jurisdictions, by enabling the bodies to recognise the work of international counterparts. Industry-focused member organisations would be well-positioned to develop this model, to involve international peers as appropriate, and to promote and raise awareness of the model among cyber assurance bodies and industry peers.

Sovereignty

In the two 'why' areas of cyber regulation, with their ties to national and economic security, governments are often highly reluctant to relinquish sovereign control. These areas lie at the core of states' fundamental responsibilities, and failing to, or appearing to fail to, take accountability and appropriate action in these areas could be politically prohibitive because these are two areas that citizens expect their governments to own. Therefore, the default response of governments when faced with challenges in this arena is to close ranks rather than open up. In addition, national cyber regulations are linked to specific domestic contexts, and this can mean that certain countries cannot align on particular requirements.

Consequently, international cooperation is something that must be fought for, rather than something that happens naturally. This dynamic can also result in a strong digital sovereignty push. In areas considered nationally sensitive (such as economic and national security), governments can seek to keep their population's data within their own borders, and they can seek to ensure that their infrastructure is controlled by domestic entities. This might mean, for example, that incident report information is kept proprietary and shared with partners only on a need-to-know basis.

To address this constraint on international cooperation, potential actions can draw on recommendations noted previously in this report. First, high-level political support, for example through the G7, would not only create a unifying banner but also send a strong signal that countries are open to international cooperation. The more parties join this effort, the more normalised cooperation becomes, and countries that pursue a solely sovereign approach to cyber regulation will be outliers that do not benefit from the advantages afforded by regulatory cooperation. Additionally, it could be worthwhile considering ways to increase accountability around the efforts participating governments are taking to cooperate internationally, for instance, by developing a channel for governments to report on the actions they are taking.

Second, generating trust through a harmonised regulation development process, as well as a shared assurance model, could help overcome countries' propensity to default to closed ranks. With increased trust, initiatives such as sharing information from incident reporting are more likely to gain traction, benefiting the wider international community. This could be used to improve the evidence base that should inform regulatory choices.

Linked to this, basing new regulations on existing international standards can support regulatory cooperation by providing a common, credible base. A range of stakeholders are naturally involved in the development of international standards, and this usually improves their applicability across various contexts as well as their quality for addressing a particular problem. This is why "anchoring in international standards" is suggested as one of the principles for a common set of good practices for developing cyber regulations.

Finally (**Recommendation X**), one approach may be to develop a mechanism that can help us to accommodate "an imperfect world": help countries adopt mostly similar approaches while retaining elements that are unique to their context. This could be done through a 'menu' of regulatory requirements. Governments would use this menu to select elements to include in their regulations, with the ambition that around eighty per cent of requirements should be similar. This menu should create commonality between jurisdictions, yet also enable countries to select options which suit their contexts. Consistent with their sovereignty ambitions, this means that countries retain a degree of control over the whole menu and specific control over the bespoke elements. At the same time, regulated organisations would have a level of certainty that no more than one-fifth of requirements in any given jurisdiction would be novel, therefore decreasing the burden of compliance.

Conclusion

While complete alignment is neither realistic nor desirable in every area, greater coherence is both achievable and needed to reduce unnecessary compliance burdens and improve security outcomes. The recommendations discussed in this Wilton Park Dialogue offer a pragmatic basis for action: strengthening common principles, achieving sustained political commitment, building trust, clarifying terminology, and creating mechanisms for accountability and collaboration. Taken together, these steps would help governments, industry, and other stakeholders move towards a more interoperable, effective, and resilient international approach to cyber regulation. The Dialogue helped to establish a shared understanding of the challenge and a practical basis for further work, with the next phase focused on taking forward implementation through clear ownership, continued collaboration, and sustained multistakeholder engagement.

Andreas Haggman
Wilton Park | June 2026

Wilton Park reports are brief summaries of the main points and conclusions of a conference. The reports reflect rapporteurs' personal interpretations of the proceedings. As such, they do not constitute any institutional policy of Wilton Park nor do they necessarily represent the views of the rapporteur. Wilton Park reports and any recommendations contained therein are for participants and are not a statement of policy for Wilton Park, the Foreign, Commonwealth and Development Office (FCDO) or His Majesty's Government.

Should you wish to read other Wilton Park reports or participate in upcoming Wilton Park events, please consult our website www.wiltonpark.org.uk.

To receive our monthly bulletin and latest updates, please subscribe to www.wiltonpark.org.uk/newsletter

Wilton Park is a discreet think-space designed for experts and policy-makers to engage in genuine dialogue with a network of diverse voices, in order to address the most pressing challenges of our time.

enquiries@wiltonpark.org.uk

Switchboard: +44 (0)1903 815020

Wilton Park, Wiston House, Steyning,
West Sussex, BN44 3DZ, United Kingdom

wiltonpark.org.uk