June 2022

G7 Common Values and Principles on Research Security and Research Integrity[1]

Vision

The 2021 G7 Research Compact states:

> We commit to promoting international research cooperation and the conditions of freedom, independence, openness, reciprocity and transparency under which it flourishes. Our governments have the right and responsibility to effectively ensure the security and integrity of the research ecosystem, in partnership with the research community, preventing the theft, misuse, and inappropriate exploitation of our intellectual property and personal data, and other forms of misconduct.

The G7 members envision the continuation of a collaborative research system where the importance of all talent – domestic and international – is acknowledged. Openness and security are not contradictory but complementary and mutually reinforcing.

To sustain this vision, we have developed and are embracing these principles of research security, which are common to the G7 members and academic communities and consistent with principles of research integrity. We will promote these principles globally.

The G7 members recognize the foundational importance of research integrity to academic discovery and research. Protecting the integrity of our research engages a broad set of considerations, including the need to implement proportionate and risk-appropriate actions in response to research security risks.

The G7 members acknowledge that there are circumstances in which it is justified to control access to research, infrastructure, or technology, and take seriously the risk of research partnerships and collaborations leading to harmful or adverse outcomes. We oppose bad-faith attempts to undermine or circumvent those access controls.

We have developed, and will continuously review, these principles for research security in collaboration with the academic community to provide a common framework, guiding responses to research security risks in domestic and international research.

Why Do Research Integrity and Research Security Matter?

Open and collaborative research underpins domestic and global responses to some of our most challenging and pressing issues. Collaborations include those with other government entities, public-private partnerships, and international science collaborations. We also recognize that collaborations can progress under a variety of formal and informal arrangements and at a variety of scales. These collaborations accelerate the pace of discoveries and increase the dynamism and openness of our research communities.

The G7 is committed to promoting open research while affirming that there are circumstances in which it is appropriate to put proportionate limits or conditions around access to research and associated data. For instance, a preliminary discovery may need protecting while researchers gather data to support publication, or controls might be placed around novel

[1] This Paper has been developed within the Sub-Working Group on Best Practice and Principles of the G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE); see Annex A for more information.

technologies for security, ethical, or commercial interests. Where research has application in military contexts, these controls are particularly important.

Some bad-faith actors choose not to respect these justified limits and seek to access and misappropriate knowledge and technology without authorization, and without recognizing or reciprocating the effort of those involved in funding or conducting the work. While such practices are driven by a variety of economic, strategic, geopolitical, or military objectives, in all cases they breach the norms and values underpinning international academic collaboration, undermine the integrity of research, and harm the security and prosperity of our societies. The G7 members oppose these practices.

At the same time, scientific advancements and their potential applications can make research a target for those who seek unauthorized access and transfer of research knowledge. These actors seek to advance their own goals and do so without recognition of – or benefit to – those involved in funding and conducting the work. While these concerning activities may be done for a variety of economic, strategic, geopolitical, or military objectives, the end results breach the norms and values that form the foundations on which international research rests, including the security and integrity of research.

As members of some of the world's most advanced economies, we play a crucial role in promoting and safeguarding the fundamental values and systems that advance science and technology and enable international scientific collaboration and innovation alongside our global scientific partners. Through the G7 Research Compact, our countries are committed to promoting international research cooperation and the conditions of academic freedom, independence, openness, reciprocity, accountability, honesty, and transparency under which it flourishes. We, in partnership with the research community, have the right and responsibility to ensure the security and integrity of the global research ecosystem is protected.

By prioritizing research security and research integrity, G7 members can ensure that the research system is protected. We can ensure that the freedom to publish results is upheld and that trust within research – and from the public in science – is maintained. We can ensure that the benefits of innovation are accredited to those who do the work and to the whole society who supports them, at the same time preventing the illicit and unethical adaptation of research results for military or national security objectives. As such, G7 members commit to ensuring that our research remains both open and secure.

What are Research Integrity and Research Security?

Research integrity is the adherence to the professional values, principles, and best practices that underpin our research communities. It forms the base on which to collaborate in a fair, innovative, open, and trusted research environment.

Research security involves the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications.

While each country may have its specific understanding of these concepts, and while it is acknowledged that these concepts continue to evolve, the G7 Working Group on the Security and Integrity of the Global Research Ecosystem (G7 SIGRE WG; see Annex A for more information) has produced working definitions for these concepts for application and adoption in line with national contexts. Figure 1 depicts how these concepts contribute to the foundation of research.

Research Integrity: Research integrity is defined for the purpose of this paper as adherence to the professional values, principles, and best practices that ensure and uphold the validity, social relevance, responsibility, and quality of research. Research integrity ensures that individuals can be confident in the advancement of research knowledge and in the dissemination of its results. While these values and principles may vary from country to country, examples include academic freedom, independence, openness, reciprocity, accountability, honesty, and transparency. These values underpin research integrity and are key to upholding the freedom of research as a universal right and public good; they are present in proposing, performing, evaluating, and reporting/disseminating research activities.

Research integrity is the foundation of research and research collaboration, domestically and internationally. The concept of research integrity – including common values, principles, legal and ethical frameworks, and best practices – is well articulated and covered by various domestic and international documents.

Research Security: As the primary focus of the G7 SIGRE WG, research security focuses on risks, activities, and behaviours that have adverse economic, strategic, and/or national and international security implications for research and that, in almost all cases, harm research integrity. Research security actions protect the integrity of research domestically and internationally, with a particular emphasis on protecting against threats to national and economic security. This includes actions that protect against the theft and misappropriation of research, as well as the unauthorized transfer of ideas, research outcomes, and intellectual property.

As a set of activities, research security encompasses:

a) The *identification* of possible risks to research by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and

b) The *activities* that protect the research inputs, processes, and the resulting ideas, research outcomes, and intellectual property, including sensitive research and personal data, from interference and misappropriation.

Disproportionate research security measures can lead to restrictions on scientific and academic freedom and openness (e.g., discouraging fruitful and positive collaborations). In worst cases, if focused on researchers of specific ethnicities, this can lead to racial profiling, and may also erode the benefits of international collaboration. On the other hand, identifying and mitigating research security risks often results in a positive impact in protecting and promoting research integrity and trust. Appropriate and risk-targeted research security measures can enhance the foundations of academic freedom, research integrity, open science, transparency, and trusted collaborations for mutual benefit.

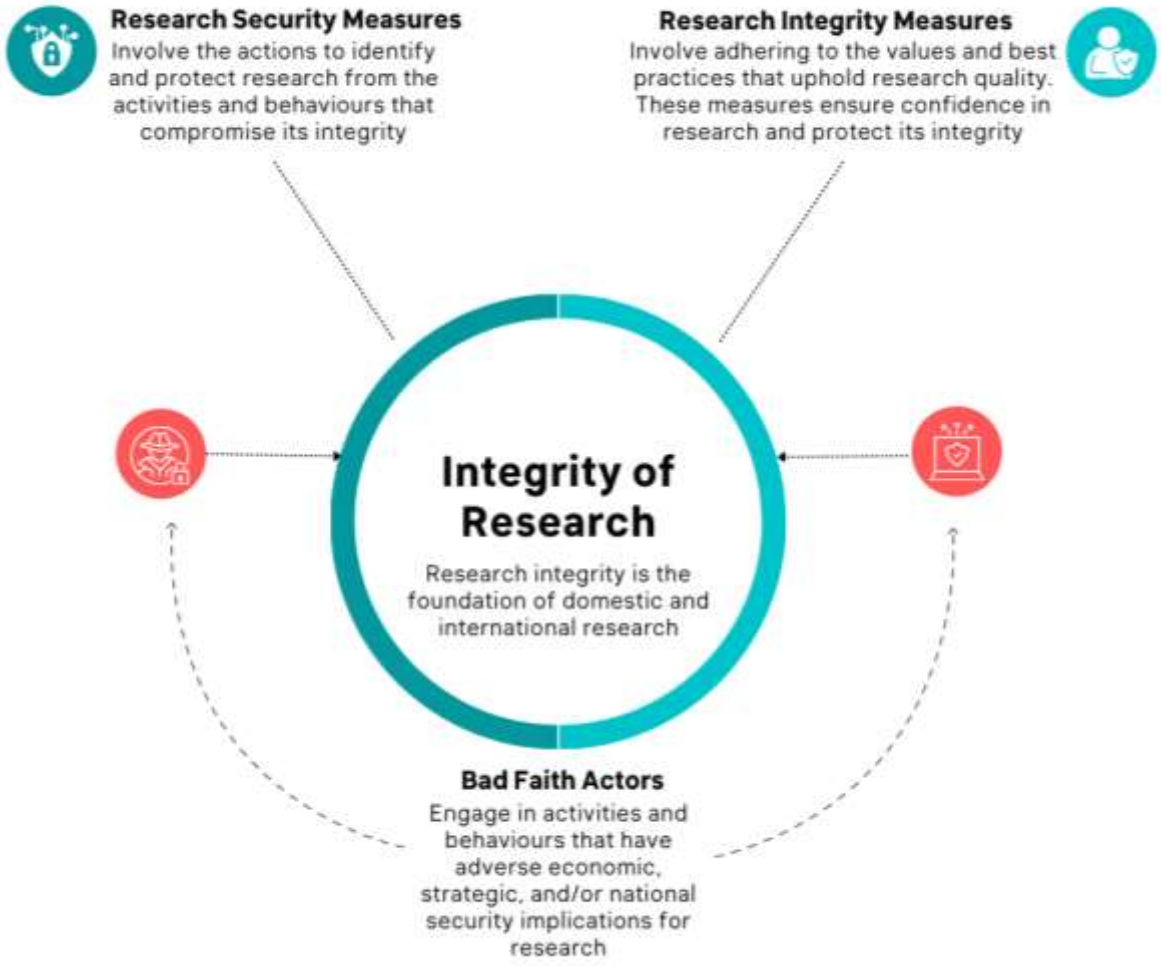

Figure 1: A graphic depicting how research security and research integrity protect the foundation of research.

Research integrity is the foundation of all research, forming the base on which to collaborate in a fair, innovative, open, and trusted environment. This is represented by the central circle. Bad faith actors use a variety of methods to undermine research integrity. These activities often include methods such as partnerships, physical access and espionage, cyber security, or insider or outsider personnel that access research; all of these activities degrade research integrity. These actions are represented by the red circles. Research security measures and research integrity measures help to protect the foundation of research and are represented by the half circles in shades of blue surrounding the integrity of research.

G7 Common Values of Research Integrity

We – the G7 members – believe the common values of research integrity apply broadly to all members of the research community, including governments, research funders, research institutions, and researchers themselves. These values include academic freedom, institutional autonomy, and the ethical conduct of research, the latter of which entails respecting the rights of those who develop ideas, research outcomes, and intellectual property throughout the lifecycle of the research project, including their publication rights.

Adherence to research integrity also includes a commitment to transparency. The open declaration of all possible conflicts of interest and conflicts of commitment – financial and otherwise – that could impact research outcomes; that may compromise public trust in research; or the selection, funding, review, or conduct of research projects. It is an essential mechanism to support both research integrity and the assessment of potential research security risks. This also extends to actions that could lead to the mismanagement of conflicts of interest and commitment, or the fabrication, falsification, plagiarism, or destruction of research data. Research integrity also entails freedom from any forms of harassment or coercion in the research process and the active promotion of equity, diversity, and inclusion.

The following list has been created by the G7 members, drawing from existing research principles and commitments, as appropriate. The list of common values is meant to articulate the shared commitment of G7 research communities, and does not establish these common values as being of equal value across all jurisdictions.

G7 members reaffirm their adherence to these common values on research integrity, in the context of research security. As G7 members look to collaboratively identify and respond to issues of research security and integrity, measures should respect and uphold the following common values on research integrity (articulated in no specific hierarchy or order):

- **Academic Freedom:** The freedom to teach, conduct, and publish research in an academic environment with an emphasis on enabling the participation of all is a fundamental tenet of research. It is fundamental to the mandate of research institutions to pursue truth, provide education to students, and disseminate knowledge and understanding. Academic freedom requires an environment of enabled autonomy and job security where researchers are free from undue external influence or limitations on scholarly inquiry.
- **Freedom from Discrimination, Harassment, and Coercion:** Freedom from discrimination, harassment, and coercion is a value that is foundational to the success of research. All members of the research community should be free from discrimination, harassment, bullying, coercion, or threats to their personal or family safety. Discrimination[2], harassment, and coercion can be by an individual, a group, an institution, or a government. This includes instances whereby entities may coerce and harass individuals to act in unethical and dishonest ways – counter to their will or interest – to support an entity's own objectives, interests, and directives.
- **Equity, Diversity, and Inclusion:** Equity, diversity, and inclusion (EDI) is the active promotion of the principles of access, diversity, and non-discrimination in all research activities – including recruitment procedures and career prospects. These are necessary for all aspects of research. EDI contributes to the diversity of identity and thought, with room for a variety of ideas, cultures, and views. Ensuring that everyone

[2] The General Conference of the United Nations Educational, Scientific and Cultural Organization deem that discrimination can be on the "basis of race, colour, descent, sex, gender, sexual orientation, age, native language, religion, political or other opinion, national origin, ethnic origin, social origin, economic or social condition of birth, or disability".

is able to freely participate in the research community, ecosystem, or enterprise will help to build an innovative, prosperous, and inclusive world.

- **Institutional Autonomy:** Research institutions can only fulfill their missions to students, faculty, staff, and society if they are free to pursue and disseminate knowledge based on evidence, data, and peer review. Institutions should be free to pursue their own missions. These missions can be based on the oversight and direction of their governance, or can be to meet community and local needs. Regardless, institutional autonomy requires a safe and secure environment in which all individuals and institutions are free and protected from unwanted external influence.

- **Open Science and Access to Research:** All members of the research community should actively support the open sharing and exchange of research results, data, methods, and inputs, while preserving the incentives for innovation. Open science – the practice of making science and research inputs, outputs, and processes available to all with minimal restrictions – should be practiced in full respect of privacy, security, and ethical considerations, as well as appropriate protection of ideas, research outcomes, and intellectual property. Enabling all members of society to build on previously validated research, open science helps to speed up the pace of new discoveries, bettering the lives of others and our societies and contributes to research quality.

- **Fostering Public Trust:** Conducting and pursuing research in a way that maintains the trust of the public and all those involved in research is vital to the continued success of science and research efforts. As contributors to integrity, all entities engaged in science and research activities should strive to demonstrate that they can meet the expectations of trust when accessing sensitive data or research. This requires deliberate, clear, and shared understandings across all partners of the purpose, use, and ownership of research results. This understanding should be upheld and respected across all stages of the research and in all jurisdictions.

  Maintaining this public trust also necessitates stewardship, which entails reflecting proper oversight and management at all levels. Governments and funding agencies have stewardship responsibilities over their decision-making and over their relationships with post-secondary institutions and research institutions. Post-secondary institutions and research institutions have stewardship responsibilities in their relationships with their employees and students, and in their communications with their sponsors.

- **Transparency, Disclosure, and Honesty:** Fully transparent and reciprocal sharing of the methods, data, and outcomes of unclassified research – while maintaining confidentiality when appropriate – is crucial to research collaboration, integrity, and the free flow of ideas and information. Transparency in disclosing researcher affiliations, competing or conflicting interests, and sources of funding is also important to ensure the integrity of the research being conducted. Transparency requires honesty. As a complementary value, honesty entails being straightforward and free of fraud and deception when proposing, developing, undertaking, reviewing, reporting, and communicating research. This extends to all aspects of research and includes the acknowledgement of the work of others and making justifiable claims or sensible interpretations based on research findings.

G7 Principles of Research Security

We – the G7 members – commit to respecting and furthering the stated research integrity common values. At the same time, we will seek to develop and implement our research security actions in line with the following research security principles.

The following list has been created by the G7 members, drawing from existing principles and commitments, as appropriate, and establishing new principles when needed. The list of principles is meant to articulate the shared commitment of G7 research communities, and does not establish these principles as being of equal value across all jurisdictions.

The following list has been created by the G7 members with the goal of clearly outlining the principles that should structure our actions and how we respond to research security risks. As G7 members look to collaboratively identify and respond to issues of research security responses should exemplify and follow these principles of research security (articulated in no specific hierarchy or order):

- **Balancing National and Global Interests:** G7 research funders and governments meet their respective and collective national, economic, and strategic interests by actively pursuing excellence in higher education, research, and innovation. At the same time, these institutions should steward and protect investments in research. Funding for scientific and research partnerships should continue to be guided by scientific merit assessments and excellence, and take appropriate and proportionate consideration and mitigation of risks to national and/or economic security where necessary. Funding should further best interests in a manner that does not compromise research integrity, looking to address global collective interests whenever possible.

- **Maintaining Openness and Research Security:** Open collaboration on research is indispensable to pushing the boundaries of innovation and addressing complex societal challenges. As a driver for greater innovation and inclusion, open science – the practice of making science and research inputs, outputs, and processes available to all with minimal restrictions – should not be an afterthought and governments should commit to making research accessible when there is no justification for it to remain closed. With benefits that include greater reproducibility of scientific results, fostering a public dialogue that engenders public confidence and trust in science, leveraging efforts, accelerating knowledge transfer and the re-use of scientific information for verifiably peaceful uses, and building synergies with international and domestic partners, governments should look to enable the open exchange of research and its results. Enhanced access and openness come with associated risks related to privacy; ideas, research outcomes, and intellectual property; national security; and public interest. As a result, this openness should be maintained to the maximum extent, acknowledging the need for safeguards for research that could have adverse ethical or national security implications.

- **Collaboration and Dialogue:** All entities involved in research should strive to support and engage with one another in the pursuit of a community that upholds security alongside openness. Researchers and institutions cannot be expected to become security experts independent of the support of those entities with the requisite expertise and knowledge. At the same time, national security organizations and governments should strive to remain receptive to the concerns and priorities of those within the research community. Governments should work collaboratively with their research communities to address domestic and international research security risks. They should commit to engaging in meaningful information sharing about the nature of the risks, with the goal of addressing common risks alongside researchers and benefiting from shared approaches. Through sustained and meaningful collaboration and

dialogue, all members of the research community can contribute to mutual and productive advancements, moving forward together.

- **Proactive Efforts:** No amount of preparation or protection can reduce the threats to research security and research integrity to zero. Recognizing this, it is not enough to react after the fact to breaches and activities that violate our shared norms and values. Governments should strive to take proactive and preventative measures that manage and reduce research security and research integrity risks based on lessons-learned and best practices. These preparations can enable all members of the research community to respond and react quickly when breaches inevitably happen, reducing their adverse impacts.

- **Risk Proportionality:** Research safeguards can have adverse impacts on innovation, partnerships, the advancement of mutually beneficial research, or result in the xenophobic treatment of others. At the same time, the likelihood of a risk occurring and the significance or magnitude of a breach can vary greatly. As a result, responses to risks should be proportionate and appropriately scaled. Risk-appropriate responses to research security should take into account the potential for misuse of the research and the aggregate level of risk, among other factors.

- **Shared Responsibilities:** No one organization can address research security on its own. At the same time, research security risks do not exist in a vacuum. To address dynamic and changing research risks, all members of the research community should acknowledge and understand their distinct roles and responsibilities with respect to addressing and managing risks to research security and research integrity. Governments should be leaders in facilitating these conversations with their respective research communities.

- **Accountability and Responsibility:** Individuals and organizations should be held accountable for all their actions, including when their behaviours deviate from accepted standards. While these standards vary across countries, being accountable entails being responsible for one's actions and for one's research from idea to publication. This also includes responsibility for research management and organization; for effective due diligence on research partners; for training, supervision, and mentoring; and for its wider impacts.

- **Adaptability:** There should be commitment to dynamic research security measures, acknowledging that overly rigid approaches run the risk of delaying beneficial research. In the absence of proportionate and flexible security measures, governments risk degrading the quality of research, leading to demotivation, a loss of benefits – such as innovation – or the forgoing of essential research pursuits altogether. Static and unwavering approaches can lead to significant disincentives and do not account for new and emerging risks.

Annex A – The G7 Security and Integrity of the Global Research Ecosystem Working Group (G7 SIGRE WG)

The G7 SIGRE WG is well-positioned to collaborate with the research community on proportionate and risk-appropriate measures that protect the security and integrity of the global research ecosystem.

This G7 SIGRE WG has three purposes as they relate to principles and best practice.

1. First, to review existing principles of research security and research integrity to understand whether they account sufficiently for security considerations. If and where they do not, the G7 SIGRE WG will develop additional principles in partnership with our respective academic communities.

2. Second, to identify voluntary standards of conduct and best practice by which such principles of research security and research integrity can be embedded.

3. Third, to strengthen the exchange of best practices across the research community around these considerations by establishing an online/virtual academy and a toolkit. The target audience for the Virtual Academy and the Toolkit should be those responsible for developing and promulgating integrity- and security-relevant policies at research funders and research-performing institutions. We have developed a persona – CRIS – which designates this audience and stands for "champions for research integrity and security.

To advance these objectives, the G7 SIGRE WG has launched a Sub-Working Group on Best Practice and Principles to produce and refine products.

The G7 Sub-Working Group on Best Practice and Principles

This Sub-Working Group consists of government, agencies, and academic representatives including representation from:

- Canada,
- Universities Canada,
- The European Commission,
- France,
- France Universités,
- Germany,
- Representatives of the Alliance of the German Science Organizations: The German Rectors' Conference (HRK), The German National Academy of Sciences Leopoldina, The Leibniz Association, The Helmholtz Association, AKIF (working group on cybersecurity of the Alliance),
- Japan,
- The University of Tokyo,
- The United Kingdom,
- Universities UK,
- The Royal Academy of Engineering,
- The United States of America,
- The Association of American Universities, and
- The University of Florida.

Given that there are significant other streams of domestic and international work occurring elsewhere on the topic of research security, this Sub-Working group *will not* look to identify a

comprehensive list of sensitive technologies that may be particularly or specifically at risk of being targeted for unauthorized knowledge transfer.

This group will look to identify existing and emerging domestic and international best practices and frameworks to address some, or all, of the vectors of research security and the behaviours and activities that have a negative impact on research security and research integrity, but *will not* look to create new frameworks to address these areas.

This group will acknowledge the relationship of domestic and international legal and regulatory frameworks that govern security (e.g., export controls, domestic laws governing higher education and research), but *will not* focus on existing legal or regulatory frameworks or measures to identify or mitigate these risks and behaviours.

As the focus of this work is the activities and risks that ultimately have a negative impact on research integrity, this group *will not* require the explicit participation of national security partners from the G7 countries.

Annex B – Research Security and Research Integrity as Evolving Concepts

Research integrity has been a key concern of the scientific community for some time and various initiatives are in place across the G7 to strengthen the integrity of global research.

While clearly established in frameworks, research integrity remains an evolving concept as risks, research environments, and the geopolitical landscape change over time; research does not occur in a vacuum, but in a complex and interconnected world.

Research security has been less concretely established in formal documents. However, as new risks emerge and grow, it is now an appropriate time to give it attention. In this work, we are cognizant that new research security risks may evolve over time and that we should adjust as necessary; there should be an opportunity to revisit these principles as time progresses.

Different countries use different terminology to describe activities to identify research security risks and measures to safeguard the research community from these risks. As research transcends borders, the G7 Security and Integrity of the Global Research Ecosystem Working Group (G7 SIGRE WG) and all associated Sub-Working Groups will work to clarify definitions and concepts in order to strengthen a common understanding of the different terminologies for evolving risks and corresponding measures to address these specific risks.

Risks and Impacts

While the drivers behind research security and research integrity concerns are distinct, in many cases the effect is to undermine key research integrity values.

The harms are often identical as well. They can include impacts on the individual researchers, including damage to professional reputations or their work, questionable research results, or a loss of reputation/publication opportunities.

Compounding this, there could be larger impacts on the research system, economy, society, and security of a country as a whole. These include the loss of value from research investments, an increase in suspicion and mistrust among and towards the scientific community and specific research findings, or inadvertent harm to others if research is used to support activities that undermine domestic or international security.

Both security and integrity risks are reduced when all those involved in research – researchers, research institutions, research funders, and governments – are properly informed about risk, understand the potential implications for their work and the research community, and can act to put in place appropriate and targeted measures to minimize these risks in a way that is governed by norms and values that are shared within the research community. It is also important to differentiate principled international collaboration, which benefits the research enterprise, from improper influence by some entities/governments that pose research security risks.

While some of the activities are the same, the G7 SIGRE WG is focused on those activities where security and research activity overlap – security-driven behaviours that ultimately impact research integrity.

How Do Individuals and Organizations Seek to Compromise Research?

Research security risks often originate across some prominent risk vectors. Individuals and organizations that look to compromise research for their own aims use a variety of methods across these vectors to engage in unwanted knowledge transfer or theft.

While this list is by no means exhaustive, it provides an effective framework for determining exactly where risks may largely originate from. These are only research security risks, but they can have an impact on research integrity, ultimately.

- **Cyber security**: Research data can be at risk of ransomware, phishing, and other cyber-attacks that take advantage of vulnerabilities in digital infrastructure or cyber security practices in order to access research data, information, or knowledge that would not otherwise be publicly available, or to compromise traditional information security objectives such as integrity, availability, and confidentiality of information.

  These methods can include supply chain attacks. These are targeted attacks on partners or suppliers of research institutions in order to better reach the actual attack target. Compromising a small supplier may be easier than directly attacking a larger and possibly better-equipped facility.

- **Physical Access and Security:** Despite the growing shift towards virtual work, the facilities where researchers undertake and store their work can also be targeted to gain access to research data, information, and knowledge.

- **Personnel:** Some parties may seek to gain and exploit access to research to serve their own undisclosed or covert interests. Insider risks come from the potential for anyone who has knowledge of, or access to, an organization's infrastructure and information and who could knowingly or inadvertently gain unauthorized access to research inputs, processes, or knowledge for illegitimate purposes.

  Some foreign states or groups use students, researchers, domestic citizens and others to acquire sensitive and proprietary information and pre-publication data and information from researchers and research entities. Often with little-to-no formal intelligence tradecraft training, these individuals wittingly or unwittingly use relatively open tools available to them to facilitate the transfer of technology and research. These are non-traditional collectors with conflicts of commitment or interest.

  There is also a risk that personnel who are not engaging in unauthorized knowledge transfer, but are lax in observing good security measures or accidentally or unwittingly provide unauthorized access to research inputs, processes and knowledge not otherwise available. States, militaries and their proxies – as well as non-state actors and organized crime organizations - could then exploit this access for their own purposes.

- **Partnerships and Collaborations**: International science and research depends on domestic and international collaborations and partnerships with individuals and organizations within and outside of academia. While the majority of partnerships are mutually beneficial and advance the reputation and standing of all involved, there are those who would use these collaborations to support unauthorized access to research inputs, processes, or knowledge for undisclosed purposes.

  By obscuring their intentions, their private commitments, or their affiliations, these research partners are misrepresenting their intentions or obscuring their reasons for partnering on specific research projects. Research partners and collaborators could have a large variation in their interests when it comes to ownership, publication, and use of ideas, research outcomes, and intellectual property, whether it is formally protected (via patents, trademarks, etc.) or not. Acquisition of, or access to, background, foreground, and other forms of research knowledge, intellectual property, or property may be used by a research partner to access additional intellectual property beyond the scope of a formal agreement and without recognition or compensation.