Rules of engagement

Restricting security-sensitive research data—a European view

Johannes Rath

The recent discussion about how to handle the results of security-relevant “dual-use” research has generated substantial polarization among stakeholders. In essence, there are two major options to prevent the abuse or misuse of research data: to restrict research itself so as to prohibit certain experiments, or to restrict the publication of research that could be abused by the military, terrorists or criminals. The case in question was the gain-of-function experiments by a research group in the Netherlands that created a strain of the H5N1 virus with increased transmissibility among mammals. The initial recommendation by the US National Science Advisory Board for Biosecurity (NSABB) was to allow only limited access to crucial data in the publications, which raised the ire of the scientific community who were concerned that their freedom of research could be curtailed in the name of security.

When a Dutch district court eventually ruled in favour of the publication of H5N1 gain-of-function research—but upheld the requirement to apply for export licences [1]—it was obvious that the final judgment over restricting the publication of security-sensitive research data will rest on the judicial system and neither on individual or collective self-governance by the research community, nor advisory boards such as the NSABB. Indeed, a key problem in finding common ground between those who are concerned about security and those who defend the freedom of research is the unresolved issue over who will have to make decisions to restrict such publications.

To resolve such controversies within EU legislation, the “Charter of Fundamental Rights of the European Union” requires the application of the Proportionality Principle. This principle pertains to both European export control legislation and research via Regulation 1291/2013, which establishes Horizon 2020, the EU’s new 90 billion Euro research framework programme. In particular, Article 19 of Regulation 1291 requires the application of the Proportionality Principle in the ethics reviews of Horizon 2020. The mandate of these reviews includes concerns related to dual use—defined as civilian versus military uses of research—and misuse, defined as terrorist and criminal use.

The Proportionality Principle is not an abstract concept. It has been an important part of European law for many decades, and courts have transformed the general principle into a structured framework to resolve value conflicts [2,3]. Applying the Proportionality Principle requires a series of tests before a final decision can be reached (Table 1). The first test, called “Means-End Test”, addresses the issue of whether the means are sufficient to accomplish the end, and it is usually broken down into two subtests. The first one, the “Effectiveness (or Suitability) Test” focuses on whether the specific action—such as restricting publication of a manuscript—is effective in accomplishing the goal: protecting society from the abuse of information therein. The second subtest, which is called the “Least Intrusive Means Test”, asks whether alternative measures are available to achieve the same goal but with fewer negative consequences. The “Means-End Test” is then followed by the “Proportionality sensu stricto Test” that uses a structured framework to balance the positive and negative consequences of the governance act.

Before applying the Proportionality Principle to the specific controversy over publishing the H5N1 gain-of-function data [4], let us consider the potential alternatives to resolving the dilemma...
between security and fundamental rights (Table 2). For many years, stakeholders have been applying risk–benefit assessments to information security measures in biosecurity-sensitive research [5]. This is due to the many institutional overlaps that exist in the governance of biosecurity with biosafety and public health and the important role of risk–benefit assessments in safety and public health.

However, the specific requirements of managing safety and security risks are sometimes contradictory. Safety officers have to inform stakeholders about the risks arising from pathogens, which requires sharing information to ensure compliance and increase awareness. Security officers in contrast often focus on limiting access to exactly the same information in order to prevent abuse or misuse. Furthermore, risk–benefit assessment relies on two prerequisites: the availability of empirical data that would enable risk managers to perform a probabilistic risk assessment, and the commensurability of risks and benefits.

In case of the publication of sequence data from H5N1 viral strains with increased transmissibility, neither prerequisite had been met at the time the decision to publish was made. Since the strain was new and artificially created, it had not been tested for its physiological properties, and therefore, the uncertainties over its biosafety- and biosecurity-relevant characteristics were high. As a consequence, the German Zentrale Kommission für Biologische Sicherheit (ZKBS; Central Commission for biological safety) based its recommendation to increase the biosafety level for work on such newly created agents to Risk Class 4 not on a risk–benefit assessment, but on the "Vorsorgeprinzip" (Precautionary Principle) [6].

Although biosecurity concerns somewhat overlap with biosafety concerns, some do not and therefore warrant additional attention in governance decisions. One of the biosecurity-specific concerns is the ability to weaponize biological agents for military or terrorist purposes. Although empirical information exists—for instance, from historical bioweapons programmes—, access to such information is generally limited. However, no such information exists for H5N1 strains from gain-of-function studies, and obtaining such information would potentially risk

| Table 1. Applying the Proportionality Principle to information security measures in research. |
|---------------------------------|---------------------------------|---------------------------------|
| **Main steps**                  | **Sub step**                    | **Question**                    |
| 1. Means-End Test              | 1.1 Effectiveness or Suitability Test | Is the applied information security measure capable of increasing security? |
|                                | 1.2 Least Intrusive Means Test  | Is the applied information security measure the least intrusive measure? |
| 2. Proportionality sensu stricto Test | 2.1 Degree of detriment of affected values | What are the negative effects of the information security measures? |
|                                | 2.2 Relevance in accomplishing a certain security level | How urgent are information security measures in the light of existing security threats? |
|                                | 2.3 Balancing                   | Are negative effects balanced with regard to gains in security? |
Table 2. Pros and cons of assessment concepts in managing information security in research.

<table>
<thead>
<tr>
<th></th>
<th>Risk–benefit assessment</th>
<th>Precautionary Principle</th>
<th>Proportionality Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity to overcome uncertainty limitations</td>
<td>Limited</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Capacity to overcome incommensurability limitation</td>
<td>Limited</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Reversal of burden of proof</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Compliance with European legal standards in handling security in a fundamental rights context</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The Precautionary Principle provides an alternative framework for overcoming the uncertainty problem. One of the most relevant versions has been introduced into EU legislation (http://europa.eu/legislation_summaries/consumers/consumer_safety/132042_en.htm), where it is used to govern environmental and safety issues; in essence, it reverses the burden of proof, leaving the affected party to provide evidence that no such risks exist. The Precautionary Principle’s main strength is its capacity to handle uncertainty in decision-making, but it still requires that priority can be given to one value over the other. Regarding environmental issues, for example, the Precautionary Principle is applied to handle uncertain and potentially irreversible environmental damage in relation to the financial interests of individuals and companies. This is different to a situation in which values such as security and fundamental rights are at stake. Given that a ranking of these incommensurable values is not foreseeable—at least not within the framework of European fundamental rights legislation—it limits the ability of the Precautionary Principle to resolve the dilemma.

How then would applying the three frameworks affect the outcome on whether or not to restrict access to information on H5N1 gain-of-function experiments? Since probabilistic-based risk–benefit assessment requires empirical data about the specific biosafety and biosecurity risks of the new virus, and since such data are not available, it cannot provide an answer about whether publication restrictions should be applied or not. Even if this limitation were overcome by acquiring relevant empirical data through testing, incommensurability problems would still limit the use of risk–benefit assessment.

The Precautionary Principle can overcome the uncertainty problem, but, as noted, we must at least be able to rank the competing values on an ordinal scale. But what should take preference? Even if we assume that security ranks higher than the other values, the reversal of the burden of proof would leave it to scientists and journal editors to prove that no relevant security risks exist to justify the restriction.

... the reversal of the burden of proof would leave it to scientists and journal editors to prove that no relevant security risks exist to justify the restriction...

The Precautionary Principle can provide a structured approach to balance negative and positive consequences. Negative impacts can be differentiated into direct effects on the freedom of information and the freedom of science, and indirect effects on public health and biosafety. Positive consequences would be either general gains in security or a response to a direct, imminent and specific threat or preparation for uncertain potential future threats. Based on the available information, it seems that the NSABB’s recommendation to restrict the publication of the H5N1 data was based on potential future uses of the sequence data and was not related to a specific security threat. Applying severe restrictions on freedom of science and freedom of speech to address uncertain future security gains raises substantial concerns about whether such restrictions are balanced and proportional.

In conclusion, restricting the publication of the gain-of-function experiments on H5N1 seems an un-proportional response. First, the proposed measure—the original recommendation by the NSABB not to publish sequence data—would have most likely not passed the Effectiveness Test. Second, it is questionable whether the recommendation represents the least intrusive measure to ensure security. Third, given the lack of specific security threats, the
marginal gains in security are not balanced by the burden on fundamental rights and principles. The decision by the Dutch export control authority to grant the licence for export and to publish the manuscript thus seems to be in compliance with the application of the Proportionality Principle.

The Proportionality Principle, in contrast to risk–benefit assessment and the Precautionary Principle, provides a suitable and practical framework to decide whether or not to invoke information security measures in biosecurity-sensitive research. Since the Proportionality Principle is the basic legal concept to resolve conflicts of fundamental rights and security in Europe, dual-use research governance must use it whenever applying security measures in order to ensure that governance measures can be upheld if challenged later in legal disputes.

Acknowledgements
I would like to thank Malcolm Dando, Alfonso García Figueroa, James A. Houghton, Ron Iphofen and Dana Perkins for the many discussions on dual use and fundamental rights that culminated in writing this manuscript.

Conflict of interest
The author declares that he has no conflict of interest.

References