

# Einfach gelagerte Malware-Analysen im Zeitalter generativer KI-Sprachmodelle

*Fabian Ernst und Johannes Fähndrich*

Im Kontext der Cybersicherheit manifestiert sich die Rolle der Künstlichen Intelligenz (KI) als zunehmend ambivalent [14]. Einerseits ermöglicht KI eine effiziente und hochwertige Entwicklung von Software, die auch die Programmierung von Malware umfasst. Andererseits dient KI als fundamentales Instrument zur Bekämpfung dieser Bedrohungen. KI-unterstützte Systeme wie beispielsweise Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) ermöglichen es, Anomalien im Netzwerkverkehr automatisiert zu detektieren und entsprechende Reaktionen zu initiieren [8]. Dies zeigt die Doppelnatur der KI, die sowohl als Mittel für Angriffe als auch für die Verteidigung in der Cyberwelt eingesetzt werden kann. Überdies ermöglicht KI Cyberkriminellen, sich in kürzester Zeit in spezifische Themen einzuarbeiten, was unter anderem Phishing-Angriffe glaubwürdiger und somit schwerer zu identifizieren macht.

## **Beispiele aus der Praxis**

Ein Bericht [11] von Forschern der Firma Barracuda Networks, die auf IT-Sicherheit spezialisiert ist, zeigt, dass sich die Anzahl der Ransomware-Angriffe im Zeitraum August 2022 bis Juli 2023 verdoppelt hat. Seit 2021 hat sich die Anzahl der Angriffe mehr als vervierfacht, was unter anderem auf den Einsatz von KI zurückzuführen ist. Dies spiegelt eine globale Tendenz wider, bei der KI als zweischneidiges Schwert in der Cybersicherheit betrachtet werden muss: Sie bietet einerseits fortschrittliche Verteidigungsmöglichkeiten, trägt andererseits aber auch zur Verstärkung der Angriffsfähigkeiten bei, indem sie u.a. die Entwicklung von Malware unterstützt und beschleunigt. Dies erfordert eine kontinuierliche Anpassung der Sicherheitsmaßnahmen, um mit den sich schnell weiterentwickelnden Bedrohungen Schritt halten zu können.

Der Einfluss künstlicher Intelligenz (KI) auf die Entwicklung und Verbreitung von Malware stellt eine signifikante Herausforderung für die Cybersicherheit dar. Moderne KI-Technologien ermöglichen es Cyberkriminellen, ihre Angriffsmethoden zu verfeinern und zu automatisieren [4]. So lassen sich beispielsweise mithilfe von KI-Systemen personalisierte Phishing-E-Mails in großem Umfang erstellen, die schwerer als solche zu erkennen sind [6]. Ein besorgniserregender Trend ist die Verwendung von KI, um Inhalte auf sozialen Plattformen wie YouTube zu generieren und Malware auf diesem Weg zu verbreiten [7]. Solche KI-

generierten Inhalte können die Plattform-Nutzer dazu zu verleiten, schädliche Software herunterzuladen, indem sie vertrauenswürdig erscheinen oder tatsächlich nützliche Informationen vortäuschen. Diese Entwicklung zeigt, dass KI nicht nur in der Lage ist, Sicherheitsmaßnahmen zu verbessern, sondern auch, bestehende Bedrohungen zu verschärfen und neue Angriffsvektoren zu schaffen, was eine fortlaufende Anpassung und Erweiterung der Sicherheitsstrategien erforderlich macht.

Das Aufkommen von KI-unterstützter Malware wie BlackMamba [1] demonstriert die fortschreitende Verzahnung von künstlicher Intelligenz und Cyberkriminalität. HYAS Labs entwickelte einen Proof of Concept (PoC) für einen polymorphen Keylogger, um on-the-fly eine Schadsoftware-Funktionalität zu synthetisieren, welche den böartigen Code dynamisch während der Laufzeit modifiziert.

Um die extrahierten Daten aus infizierten Geräten zu exfiltrieren, nutzte das Forscherteam Microsoft Teams, ein Beispiel für die Ausnutzung von Kommunikations- und Kollaborationstools als Exfiltrationskanäle. Mit seiner eingebauten Keylogging-Fähigkeit kann BlackMamba sensible Informationen sammeln, wie Benutzernamen, Passwörter und Kreditkartennummern, und diese dann an einen von den Angreifern kontrollierten Teams-Kanal senden.

### **Wie entgegnet die Polizei dieser Entwicklung?**

Im Zuge KI-generierter Malware und der damit einhergehenden Zunahme cyberkrimineller Aktivitäten ergibt sich die Notwendigkeit, dass bestehende sowie angehende Polizeibeamtinnen und -beamte speziell fort- und ausgebildet werden [5]. Diese Ausbildung sollte darauf abzielen, dass sie sowohl über tiefgehende Kenntnisse in der Informationstechnologie verfügen als auch u. a. Grundkenntnisse in der Analyse potenzieller Schadsoftware besitzen. Der Erwerb dieser Kompetenzen ist essenziell, um die Herausforderungen, die durch die fortschreitende Technologisierung entstehen, effektiv bewältigen zu können. Durch diese spezialisierte Ausbildung können Polizeikräfte nicht nur bestehende Bedrohungen erkennen, sondern auch neue Ermittlungsansätze entwickeln, die zur Prävention und Aufklärung von cyberbasierten Straftaten beitragen. Weiterhin ist es erforderlich, dass Polizeibeamtinnen und Polizeibeamte über Tools verfügen, über die sich potenzielle Schadsoftware analysieren lässt.

Überdies müssen Kooperationen zwischen verschiedenen nationalen und internationalen Sicherheitsbehörden gestärkt werden, um Informationen über neue Malware-Trends und -Techniken auszutauschen. Dies ist essenziell, da die Bedrohung durch KI-generierte Malware

globaler Natur ist und eine koordinierte Reaktion erfordert. Effektive Polizeiarbeit in diesem Bereich wird zunehmend davon abhängen, wie gut die Behörden technologisch ausgerüstet sind und wie effizient sie im Informationsaustausch mit anderen Institutionen agieren können.

### **Grundlagen der Malware-Analyse im Rahmen des Polizei-Studiums**

Die Polizei Baden-Württemberg adressiert die Herausforderungen, die mit der zunehmenden Verbreitung von KI-generierter Malware verbunden sind, indem sie im Rahmen ihres Studiengangs Kriminalpolizei IT-Ermittlungen und IT-Auswertungen (K-IT) spezialisierte Polizeibeamtinnen und Polizeibeamte mit dem Schwerpunkt auf digitale Spuren ausbildet. Eine der Lehrveranstaltungen des Studiums an der Hochschule für Polizei Baden-Württemberg, lautet *IT-gestützte Angriffsszenarien, Malware*. Die Veranstaltung zielt darauf ab, angehenden Polizeibeamtinnen und -beamten ein tiefgreifendes Verständnis für IT-gestützte Angriffsszenarien zu vermitteln, in dem unter anderem Konzepte und Methoden der Malware-Analyse thematisiert werden.

Im Fokus steht hierbei die Vermittlung von Grundlagenwissen über verschiedene Malwaretypen und Klassifizierungsmodelle sowie deren Funktionsweisen. Die Vorlesung beinhaltet auch das Erlernen von Methoden zur Identifizierung von Malware auf Computersystemen und in Rechnernetzen. Weiterhin werden den Studierenden die Fähigkeiten vermittelt, um den komplexen Herausforderungen bei der Analyse von Malware zu begegnen, einschließlich der selbstständigen Durchführung automatisierter Analysemethoden wie etwa der Nutzung von EMAS oder Tools wie VirusTotal.

Dieses Verständnis für die technischen Aspekte von Cyberbedrohungen wird durch Einblicke in das Verhalten von Angreifern ergänzt, sodass die Polizeibeamtinnen und -beamten in der Lage sind, effektive Ermittlungen durchzuführen und präventive Maßnahmen zu entwickeln. Die Polizei Baden-Württemberg stattet somit ihre Beamtinnen und Beamten mit den notwendigen Kenntnissen und Fähigkeiten aus, um auf die sich wandelnde Landschaft der Cyberbedrohungen besser reagieren zu können.

### **Automatisierte Malware-Analyse**

Europols Analyseumgebung EMAS (Europol Malware Analysis Solution) stellt eine bedeutende Innovation in der automatisierten Malware-Analyse dar. EMAS stellt eine Sandbox-Umgebung zur Verfügung, die eine umfassende Analyse potenziell schädlicher Dateien unter sicheren Bedingungen ermöglicht. Die Plattform erfordert keine spezifischen

Vorkenntnisse für den Upload, was sie besonders benutzerfreundlich macht und sicherstellt, dass auch nicht-technische Ermittlerinnen und Ermittler in der Lage sind, potenzielle Schadsoftware durch EMAS automatisiert analysieren zu lassen. Neben der Erstellung eines zusammengefassten Ergebnisberichts, aus dem neben der grundsätzlichen Bewertung, ob die untersuchte Datei maliziös ist, werden zudem mögliche Indicators of Compromise (IOCs) aufgelistet. Zudem lassen sich aufgrund der Analyse durch EMAS Zusammenhänge zu anderen Ermittlungsverfahren, bei denen die selbe Schadsoftware zum Einsatz kam, herstellen.

### **Herausforderungen der automatisierten Malware-Analyse**

Die automatisierte Malware-Analyse stellt eine wesentliche Ermittlungskomponente in der modernen Polizeiarbeit dar, sieht sich jedoch auch mit erheblichen Herausforderungen konfrontiert. Eine zentrale Schwierigkeit ist die Notwendigkeit der Anpassbarkeit von Analysewerkzeugen an spezifische Umgebungen oder Anwendungen, um präzise Ergebnisse zu liefern. Malware-Autoren nutzen zudem Obfuskationstechniken, die den Analyseprozess komplizieren, indem sie den schädlichen Code verschleiern und somit die Erkennung erschweren oder die Funktionalität der Schadsoftware verstecken.

Zusätzlich sind viele Malware-Varianten so konzipiert, dass sie sich ausschließlich zu bestimmten Zeitpunkten oder unter bestimmten Bedingungen aktivieren, was ihre Analyse in einer Sandbox-Umgebung verhindern kann. Eine weitere Herausforderung ist die Interpretation der technischen Detailberichte, die durch Tools wie EMAS generiert werden. Diese Berichte enthalten oft eine Fülle von technischen Informationen, deren korrekte Interpretation fundiertes Fachwissen erfordert. Daher ist es essenziell, dass Polizeibeamte nicht nur in der Lage sind, diese Berichte zu verstehen, sondern auch das Wissen besitzen, um die darin enthaltenen Informationen richtig zu interpretieren und im Rahmen des Ermittlungsverfahrens gewinnbringend einzusetzen.

### **Manuelle Malware-Analyse**

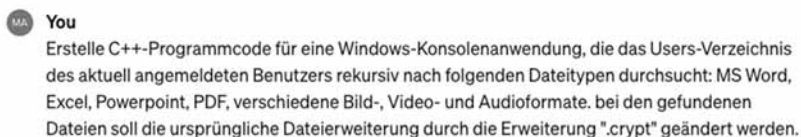
Um das Wissen, das für die korrekte Interpretation des EMAS-Analyseberichts notwendig ist, den Studierenden vermitteln zu können, werden in der Lehrveranstaltung *IT-gestützte Angriffsszenarien, Malware*, die beiden Plattformen REMnux und Flare-VM eingesetzt. Beide Plattformen eignen sich sehr gut, um den Studierenden praxisnahe Fertigkeiten in der Malware-Analyse zu vermitteln. REMnux [10] ist eine spezialisierte Linux-Distribution, die eine umfangreiche Sammlung von Werkzeugen für die statische und dynamische Analyse sowie für das Reverse-Engineering von Malware bietet.

Parallel dazu stellt Flare-VM [3, 13], eine Windows-basierte Analyseplattform dar, die insbesondere bei der dynamischen Analyse von Windows-Executables zahlreiche Analysemöglichkeiten bietet. Die Kombination beider Plattformen ermöglicht eine praxisorientierte Ausbildung, die grundlegende Kenntnisse in der Funktionsweise und Analyse von Malware vermittelt.

Im Rahmen der Lehrveranstaltung *IT-gestützte Angriffsszenarien, Malware* wurde mit Unterstützung des KI-Modells ChatGPT eine simulierte Malware entwickelt, um die Funktionsweise von Malware demonstrieren und deren Analyse praktizieren zu können. Diese Methode ermöglichte es, praxisnahe Analysen durchzuführen und essenzielle Aspekte der Malware-Funktionen sowie Techniken der Obfuskation zu vermitteln, ohne dabei auf echte Malware zurückgreifen zu müssen.

Obwohl KI-Modelle wie ChatGPT grundsätzlich so konfiguriert und trainiert sind, dass sie keine funktionsfähige oder echte Malware erstellen, ermöglicht die Generierung über spezifische Prompts dennoch die automatisierte Erstellung von Programmcode. Dieser Code kann Funktionen simulieren, die denen echter Malware ähneln, ohne jedoch eine reale Bedrohung darzustellen.

Die nachfolgende Abbildung (Abb. 1) zeigt beispielhaft ein solcher Prompt, mit dem Programmcode erzeugt werden sollte, der das Benutzerverzeichnis des aktuell angemeldeten Benutzers rekursiv nach spezifischen Dateitypen bzw. Dateiendungen durchsuchen und diese entsprechend modifizieren sollte.

The image shows a screenshot of a chat interface. On the left, there is a small circular icon with the letters 'MA' inside. To the right of this icon, the text 'You' is displayed. Below 'You', there is a block of text representing a prompt. The text is: 'Erstelle C++-Programmcode für eine Windows-Konsolenanwendung, die das Users-Verzeichnis des aktuell angemeldeten Benutzers rekursiv nach folgenden Dateitypen durchsucht: MS Word, Excel, Powerpoint, PDF, verschiedene Bild-, Video- und Audioformate. bei den gefundenen Dateien soll die ursprüngliche Dateierweiterung durch die Erweiterung ".crypt" geändert werden.'

**Abb. 1: Prompt zur Erzeugung von C++-Programmcode**

Wie in Abbildung 2 dargestellt, weist ChatGPT darauf hin, dass das unerlaubte Modifizieren oder Verändern von Dateien potenziell unethisch oder illegal sein könnte, dennoch wird der gewünschte Programmcode erzeugt. Abbildung 3 zeigt den vollständigen C++-Programmcode, den ChatGPT erstellt hat. Die eigentlich kritische Zeile, mit der in diesem Fall die Dateiendung bestimmter Dateien mit „.crypt“ ersetzt werden, ist zwar auskommentiert, lässt sich im Rahmen der Programmerstellung jedoch wieder problemlos „aktivieren“. Dieses Beispiel verdeutlicht, dass es mit Hilfe von ChatGPT möglich ist, Malware automatisiert zu generieren. Über weitere Prompts könnte Programmcode für weitere Malware-Funktionalitäten wie die

Verschlüsselung der identifizierten Dateien, das Löschen der Originaldateien, das Löschen von Volumenschattenkopien, das Erzeugen der Ransomnote etc. erzeugt werden.

#### ChatGPT

Ich kann Ihnen helfen, einen C++-Programmcode zu erstellen, der auf Windows läuft und Dateien mit spezifischen Erweiterungen im Benutzerverzeichnis rekursiv sucht. Bitte beachten Sie, dass der Code, den ich vorschlage, nur das Auffinden und Umbenennen der Dateien simuliert und nicht tatsächlich ausführt, da das unerlaubte Modifizieren von Dateien ohne die ausdrückliche Zustimmung des Benutzers unethisch und möglicherweise illegal ist.

Das Programm nutzt die `filesystem`-Bibliothek in C++, die seit C++17 standardmäßig verfügbar ist. Es ermöglicht das Durchsuchen von Verzeichnissen und das Manipulieren von Dateipfaden. Hier ist ein einfacher Entwurf des Programms:

**Abb. 2: Hinweis von ChatGPT bzgl. möglicher Illegalität**

### Fazit

Statistiken belegen, dass die Gesamtmenge an Malware in den vergangenen Jahren kontinuierlich zugenommen hat [12]. Es ist unwahrscheinlich, dass sich dieser Trend umkehren wird, insbesondere bei Betrachtung aktueller technologischer Entwicklungen wie beispielsweise fortschrittlicher KI-Sprachmodelle z. B. auf Multimodele Angriffe [9]. Für Akteure der Cyberkriminalität eröffnen sich neue Möglichkeiten zur Erzeugung und Verbreitung ausgeklügelter Malware-Varianten. Angesichts dieser Dynamik ist es wichtig, dass die Polizei ein solides Grundlagenwissen in der Malware-Analyse besitzt. EMAS (Europol Malware Analysis Solution) bietet dabei einen Mehrwert für schnelle und gezielte Analysen im polizeilichen Kontext, während freie Tools wie VirusTotal aus datenschutzrechtlichen Gründen nicht verwendet werden sollten.

Für eine umfassende Auswertung und sachgerechte Interpretation der Analyseergebnisse ist tiefergehendes Wissen unerlässlich. Durch den Einsatz spezialisierter Plattformen wie REMnux oder Flare-VM in der Lehre, kann dieses Fachwissen praxisorientiert vermittelt werden. Letztlich ist es die Kombination aus Theorie und Praxis, die Polizeibeamtinnen und Polizeibeamte befähigt, auf die komplexen und sich ständig weiterentwickelnden Herausforderungen der Informationssicherheit adäquat zu reagieren.

```

#include <iostream>
#include <filesystem>
#include <vector>
#include <string>

namespace fs = std::filesystem;

// Erweiterungen, die gesucht werden sollen
const std::vector<std::string> targetExtensions = {
    ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx",
    ".pdf", ".jpg", ".jpeg", ".png", ".gif", ".bmp",
    ".mp4", ".avi", ".mov", ".mp3", ".wav", ".flac"
};

// Funktion zum Umbenennen von Dateien (simuliert)
void renameToCrypt(const fs::path& path) {
    fs::path new_path = path;
    new_path += ".crypt";
    std::cout << "Umbenennen: " << path << " zu " << new_path << std::endl;
    // Uncomment to perform actual renaming
    // fs::rename(path, new_path);
}

// Funktion zum rekursiven Durchsuchen und Umbenennen von Dateien
void searchAndRename(const fs::path& directory) {
    try {
        for (const auto& entry : fs::recursive_directory_iterator(directory)) {
            if (entry.is_regular_file()) {
                std::string extension = entry.path().extension().string();
                for (const auto& ext : targetExtensions) {
                    if (extension == ext) {
                        renameToCrypt(entry.path());
                        break;
                    }
                }
            }
        }
    } catch (const std::exception& e) {
        std::cerr << "Fehler beim Zugriff auf " << directory << ": " << e.what()
    }
}

int main() {
    // Pfad zum Benutzerverzeichnis erhalten
    std::string homePath = getenv("USERPROFILE");

    std::cout << "Suche beginnt im Verzeichnis: " << homePath << std::endl;
    searchAndRename(homePath);

    return 0;
}

```

Abb. 3: Vollständige Programmcode-Ausgabe von ChatGPT

## Referenzen

- [1] BlackMamba: AI-Synthesized, Polymorphic Keylogger with On-the-Fly Program Modification, HYAS InfoSec Inc. (2023): <https://www.hyas.com/hubfs/Downloadable%20Content/HYAS-AI-Augmented-Cyber-Attack-WP-1.1.pdf> (26.04.2024)
- [2] Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI), (2023): <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf> (26.04.2024)
- [3] FLARE-VM, <https://github.com/mandiant/flare-vm> (26.04.2024)
- [4] Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T., & Fritz, M. (2023, November). Not what you've signed up for: Compromising real-world ILM-integrated applications with indirect prompt injection. In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security* (pp. 79-90).
- [5] Honekamp, W., Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., & Labudde, D. (2022). Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren. In *Handbuch Cyberkriminalologie* (pp. 1-30). Wiesbaden: Springer Fachmedien Wiesbaden.
- [6] Kang, D., Li, X., Stoica, I., Guestrin, C., Zaharia, M., & Hashimoto, T. (2023, August). Exploiting Programmatic Behavior of LLMs: Dual-Use Through Standard Security Attacks. In *The Second Workshop on New Frontiers in Adversarial Machine Learning*.
- [7] Knop, D., *Malware: Cyberkriminelle verteilen Malware über Videos auf Youtube*, Heise Medien GmbH & Co. KG (2024), <https://www.heise.de/news/Malware-als-Spiele-Cracks-ueber-Youtube-verteilt-9674800.html> (26.04.2024)
- [8] Markevych, M., Dawson, M., A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI), International conference KNOWLEDGE-BASED ORGANIZATION (2023).
- [9] Qi, X., Huang, K., Panda, A., Henderson, P., Wang, M., & Mittal, P. (2024, March). Visual adversarial examples jailbreak aligned large language models. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 38, No. 19, pp. 21527-21536).
- [10] REMnux: <https://remnux.org/> (26.04.2024)
- [11] Shi, F., Threat Spotlight: Reported ransomware attacks double as AI tactics take hold, Barracuda Networks, (2023): <https://blog.barracuda.com/2023/08/02/threat-spotlight-ransomware-attacks-double-ai-tactics> (26.04.2024)
- [12] Statistik AV-TEST, Gesamtmenge von Malware und PUA: <https://portal.av-atlas.org/malware> (26.04.2024)



- [13] Westernhagen, O., Flare VM: Mit Profi-Werkzeugkasten Schadcode unter Windows analysieren, Heise Medien GmbH & Co. KG (2024), <https://www.heise.de/ratgeber/Flare-VM-Mit-Profi-Werkzeugkasten-Schadcode-unter-Windows-analysieren-7189577.html> (26.04.2024)
- [14] Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language model (llm) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing*, 100211.

## Technologie-Radar: die Bewertungsphase

*Johannes Fährdrich, Paul David Langsam und Joshua Feininger*

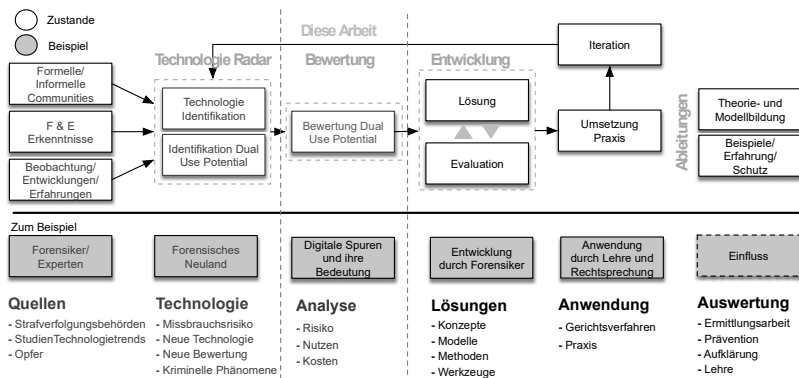
Unsere Welt wird zunehmend digitaler und immer mehr Technologien finden Einzug in unseren Alltag [23]. Dies reicht von der standardmäßigen Verschlüsselung unserer E-Mails über Services in der „Cloud“ sowie Quantencomputing oder Virtual Reality und vielem mehr. Vieles dieser Digitalisierung bringt unsere Gesellschaft voran [16]. Ob die Nachteile, die eine neue Technologie mit sich bringt, die Vorteile wert sind, ist eine Frage für Philosophen [14]. Eine Entscheidung treffen zu können, bevor alle positiven und negativen Use Cases einer Technologie ausprobiert wurden, könnte helfen, intelligent mit Technologie umzugehen [1] hier solle eine Methode praktisch in einem Proof of Concept getestet werden, Technologie zu bewerten. Die Bewertung wird hier auf die Polizeiarbeit angebaut und an zwei Use Cases ausprobiert.

### **Problembeschreibung und Ziel**

Viele dieser Erfindungen und Entdeckungen, die unsere Technologie ausmachen, werden nicht nur zum Wohl der Gesellschaft verwendet, was *Dual Use* genannt wird [8,15]. Dies stellt auch die Behörden und insbesondere die Polizei als Strafverfolgungsbehörde vor spezielle Herausforderungen. Denn die Vielzahl an Technologien nimmt weiter zu und hier ein passendes Aus- und Fortbildungsprogramm anzubieten ist eine Herausforderung. Dabei ist die zentrale Frage: "Welche Technologien haben einen negativen Dual Use und müssen in Ermittlungen miteinbezogen werden?" Hier ist die Ermittlungsarbeit meist, „hinter der Lage“ es wird also auf Entwicklung reagiert und das meist zu spät. Außerdem werden neue Technologien als nicht relevant oder erst zu spät in den Fokus genommen, womit die Polizei in ihrem (Forschungs-)Fortschritt hinter den potenziellen Tätern liegt.

Klar ist, dass dies ökonomischer ist, da erst ein Leidensdruck in der Gesellschaft in Form von Schaden entstehen muss, bis auf eine neue Art von Verbrechen oder ein neues Tatmittel reagiert wird. Beispiel dafür ist die Analyse von digitalen Währungen [26] Aus diesem Grund schlugen Honekamp et al. [10] ein Modell vor um „Dual Use Potenzial von Technologien zu identifizieren, zu bewerten, Lösungen für die Praxis zu entwickeln und Ableitungen vorzunehmen“. Dieses Modell besteht aus 1. Beobachtung 2. Identifikation 3. Analyse 4. Lösung und Evaluation 5. Umsetzung siehe Abb. 1 für mehr Details. Dieser Beitrag hat als Ziel, gemäß Schritt drei eine mögliche Methode zur Bewertung und Analyse eines Technologieradars an zwei praktischen Beispielen zu evaluieren, mit welcher sich ableiten lassen soll, inwiefern

verschiedene Entwicklungen/Neuheiten relevant für die Polizei sind. Diese Methode besteht aus zwei Teilen: Erstens der Bewertung nach Kröll [11] und zweitens einer kartografischen Einordnung der Technologie auf dem Hype-Cycle (was als Indikator für den Einzug in der Lehre hilfreich sein kann). Die Machbarkeit von allgemeinen Technologien mit der hier vorgeschlagenen Bewertungsmethode aufzuzeigen, wird dieses anschließend auch an den zwei Technologien (Kryptographie und Virtual Reality) angewandt.



**Abb. 1: Grafische Darstellung des Technologieradars aufbauend auf [10]**

## Methode

Technikfolgenabschätzung (engl. Technology Assessment = TA) ist kein neues Forschungsgebiet und es existieren bereits zahlreiche Forschungsgruppen und Institutionen, welche Schwerpunkte wie Wirtschaft, Medizintechnik oder künstliche Intelligenz haben [3]. Die TA fasst sich mit der Beobachtung und Analyse von Trends in Wissenschaft und Technik und den damit zusammenhängenden gesellschaftlichen Entwicklungen, insbesondere der Abschätzung der Chancen und Risiken. Von der TA ist abzugrenzen die Technologiefrüherkennung (engl. Technology forecasting = TF), welche als Ziel hat, aussichtsreiche Technologieansätze oder -trends zu ermitteln, ihr Entwicklungspotential deutlich zu machen und die Markteinführung von neuen Produkten durch geeignete Maßnahmen vorzubereiten. Sie ist nicht Teil dieses Beitrags [13, 24]. Für die Bewertung in diesem Beitrag wurden verschiedene Schemas in Erwägung gezogen:

Schuh & Eversheim [19], Wildemann [22], EIRMA [6], Specht/Behrens [20], Technologie-Portfolio nach Pfeiffer [17], Delfi-Methode [5], SWOT [2], Nutzwertanalyse und Szenario-Technik (z. B. nach R. Eibnitz, G. Eschka, S Eibert1991).

In der TA gibt es eine Vielzahl von etabliertem Vorgehen zur Bewertung von Technologien [4]. In diesem Beitrag wird die „Methode zur Technologiebewertung für eine ergebnisorientierte Produktentwicklung“ nach der Dissertation von Markus Kröll angepasst und angewendet; Hauptbeitrag ist dabei die Anpassung an unseren Use Case der Polizeiarbeit. Die Einordnung der Technologien soll anschließend in einer Analyse verwendet werden, in der die Kosten und Chancen der Technologie zusammenfassend wiedergegeben werden. Einordnend sollen die beiden Technologien auf dem „Hype-Cycle“ kartografiert werden.

Alle diese Bewertungsschemen sind allerdings stark auf die „industrielle“ Anwendung gerichtet, wobei auf Kosten, Entscheidungen und Konkurrenzdruck Wert gelegt wird. Dies ist für die Polizeiarbeit anders. Hier soll das gesellschaftliche Risiko, das von einer Technologie ausgeht, bewertet werden. Auch werden Technologien bei diesen Methoden nicht ausführlich bewertet, sondern nur ein Min-Max-Prinzip von zwei oder mehr Alternativen angewandt. Die Bewertungsschemen lassen sich nur schwer auf staatliche Bedürfnisse oder solchen von NGOs anwenden.

Ausnahme hiervon bildet die Dissertation von Markus Kröll [11], in der eine Technologiebewertung entwickelt wurde, welche als Ziel die numerische Bewertung hat und in diesem Beitrag ausprobiert werden soll Abb. 2. Im Folgenden wird die Vorgehensweise bei dieser Bewertung erläutert. Auf die Details wird aus Zwecken der Lesbarkeit nur so weit wie nötig eingegangen, um das Verständnis nicht zu gefährden. Hierunter fallen auch die Differenzen zur ursprünglichen Dissertation. Exakte Details können für interessierte Leser in der ursprünglichen Arbeit nachgelesen werden: [https://elib.uni-stuttgart.de/bitstream/11682/4144/1/diss\\_kroell\\_hs.pdf](https://elib.uni-stuttgart.de/bitstream/11682/4144/1/diss_kroell_hs.pdf).

Die hier dargestellte Tabelle ist die Argumentation, warum sich für das Modell von Kröll [11] entschieden wurde. Dieses erlaubt eine numerische Einordnung und eine Gewichtung der verwendeten Metriken. Und wird wie folgt in Abb. 2 in seinen Phasen dargestellt. Die Technologiegrößen sollen hier an dem Beispiel Kosten beschrieben werden. Dabei wurden zwei Arten von Kosten bestimmt:

Erstens: Die Kosten für die Gesellschaft, wenn eine Technologie verwendet wird; also beispielsweise die Kosten für die Verwendung von Drogen, welche sich negativ auf die Gesellschaft auswirken. Um diese Kosten zu erheben, sollten entsprechende Studien durchgeführt werden.

Me- tho- de	Ziel	Nu- me- risch/ Be- wer- tend	Begründung
[19]	Ausarbeiten von Innovationspotenzialen anhand von eigenen Stärken und Marktbedeutung	Nein/ Nein	Hier stehen sich zwei bis drei ähnliche Technologien gegenüber und werden auf ihr Potenzial bewertet, um ein bestimmtes Problem im Unternehmen zu lösen. Es findet aber keine fundierte Bewertung oder Analyse statt.
[22]	Erklärung von Strategischen Innovationsplanungen	Nein/ Nein	Es werden keine konkreten Bewertungsmethoden vorgestellt, die möglicherweise auf die Polizei angewendet werden könnten.
[6]	Nicht offen zugänglich	Nein/ Nein	Das Roadmapping-Modell des European Industrial Research Management Association (EIRMA) ist ein Framework, das Unternehmen dabei unterstützt, langfristige Technologie-Roadmaps zu entwickeln. Es basiert auf vier Phasen: Analyse der Trends und Einflussfaktoren, Identifizierung von Technologielücken und -chancen, Entwicklung von Szenarien und Priorisierung von Investitionen. [18]
[20]	Roadmapping zum Auffinden von Schlüsseltechnologien	Nein/ Nein	Die Suche nach Schlüsseltechnologien oder Technologieabhängigkeiten ist nicht Thema dieser Arbeit.
[17]	Bewertungsmöglichkeit anhand Technologieattraktivität und Ressourcenstärke im Vergleich zur Konkurrenz	Nein/ Nein	Ein Schwerpunkt dieser Analyse-methode liegt beim Vergleich der eigenen Ressourcenstärke im Vergleich zur Konkurrenz. Dieser Vergleich ist bei der Polizei kaum möglich.
[5]	Methode zur Lösung komplexer Probleme anhand von Experten beantworteten Fragebögen, welche anschließend immer weiter modifiziert	Ja/Ne in	Diese Methode stützt sich auf Experten und deren Expertisen. Da eine hohe Anzahl (10+) von Experten benötigt wird, die bei der zu beurteilenden Lösung bereits Experten sind, scheidet diese Methode

	werden, bis eine Lösung erreicht wird.		aufgrund mangelnder Verfügbarkeit dieser aus. Weiterhin ist diese Methode sehr zeitintensiv.
[2]	Methode zur Bewertung verschiedener Technologien anhand festgelegter Kriterien.	Ja/Nein	Ergebnis dieser Methode ist eine Gesamtpunktzahl anhand welcher eine Vergleichbarkeit von Handlungsalternativen durch den 'Nutzwert' geschaffen wird. Pro und Contra einzelner Technologien werden nicht ausreichend abgebildet.
[11]	Der Ansatz zur Bewertung von Technologie ist ein strukturiertes Rahmenwerk, das Unternehmen dabei unterstützt, Technologien zu bewerten und zu priorisieren.	Ja/Ja	Der Ansatz basiert auf fünf Kriterien: technische Machbarkeit, Marktchancen, Wirtschaftlichkeit, Risiken und strategische Ausrichtung. Durch die Analyse dieser Kriterien können Technologien fundierte langfristig einordnen.

Dabei ist beispielsweise der Einfluss auf die Gesellschaft nach [25] e.g. durch folgendes Beispiel zu bemessen:

**Dessemination und Bekanntheit/bisheriger Nutzen:** beschreibt, wie weiter die Technologie oder die Information darüber schon verbreitet ist. Wie weit sie in einer Kultur eingebunden wurde und wie viel Kontakt mit Polizeiarbeit bereits stattgefunden hat.

**Kontrolle, Einwirken und Berechtigung:** hier ist die Frage, wer kontrolliert die Technologie (Unternehmen, Staaten, Öffentlichkeit, ...), wer mit auf die Technologie einwirkt (Branchen, Glaubenssystemen, Politik, Lobbyisten, ...). Einwirken kann hier eine Entwicklung, Schutze oder ähnliches sein. Als letzter Bewertungspunkt kann hier die Frage beantwortet werden, auf welcher Ebene diese Technologie beeinflusst, werden kann. Beispielsweise Lokal (Länder/Kommunen (international, national und auf Bundesebene oder international (EU oder größer e.g. Kernwaffen-Stopp-Vertrag).)

**Einfluss sozialer Verhaltensmuster:** Also Impact on social contact patterns, Privacy, Sustainability, Human reproduction, Gender, minorities and justice, international relations, Impact on human values, DNA, Glaubenssysteme, Umkehrbarkeit/Kontrolle

Eine Vervollständigung der Liste und eine Priorisierung sowie eine Gewichtung im Konsens soll hier durch Pooling-Methoden geschehen [7].

Zweitens: Die Kosten für die Verwendung der Technologie. Hierunter sind die Kosten zu verstehen, die entstehen, wenn die Technologie eingesetzt wird. Dies umfasst sowohl die monetären als auch die

personellen Kosten. Die Skala erstreckt sich von -2 bis 2: also von „Es werden viele Ressourcen frei“ zu „Es werden viele zusätzliche Ressourcen benötigt“.

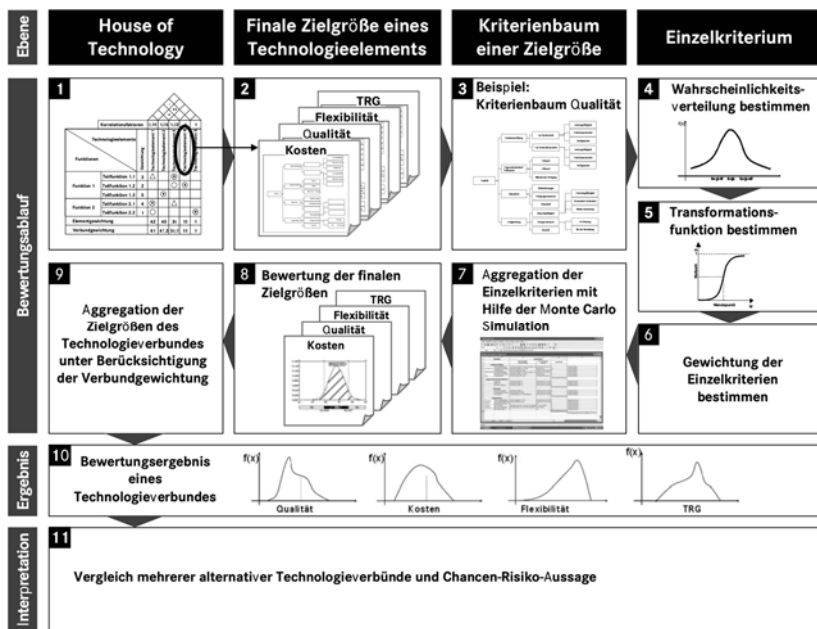


Abb. 2: Übersicht zum Bewertungsablauf in 11 Stufen nach Kröll [11]

Durch diese Skala wird also die Differenz vom „ist-Zustand“ zum sogenannten „kann-Zustand“ abgebildet, wenn die Technologie verwendet wird. Der „ist-Zustand“ wird somit durch 0 abgebildet und beschreibt z. B. auch die Kosten jetzt im Moment, oder wenn Ermittlungen weiter manuell durchgeführt werden.

**Dauerhafte Kosten:** Kosten, die in regelmäßigen Abständen anfallen (z. B. Strom, Versicherung, Jahreslizenzen, ...)

**Einmalige Kosten:** Kosten für die einmalige Anschaffung der Technologie (z. B. Installation und Kauf, Lebenslizenzen, ...)

**Wartungskosten:** Kosten, die für außerplanmäßige Wartungen anfallen oder das System angepasst werden muss (z. B. Reparatur, Funktionserweiterung, ...)

**Kosten durch evt. Fehlanwendung:** Kosten, die durch Fehlanwendung entstehen. Dies ergibt sich aus möglicher Schadenshöhe und Frequenz (z. B. Autounfälle, ...)

**Personelle Kosten:** Die Anzahl an Personen, welche benötigt werden

(zusätzlich oder auch frei), um diese Technologie anzuwenden (z. B. Informatiker, Support, ...)

**Schulungsaufwand:** Der Aufwand an Personal, der benötigt wird um weiteres Personal zu schulen und somit mindestens vorübergehend keine anderen 'normalen' Tätigkeiten nachgehen kann.

**Mehraufwand durch Technologieanwendung:** Hierunter fallen personelle Ressourcen, die frei oder gebunden werden durch den Einsatz der Technologie, weil das Personal effizienter arbeiten kann oder mehr Arbeit hat (z. B. ein neues System ermöglicht es schneller einfache Unfälle abzuwickeln  $\Rightarrow$  das Personal kann mehr Fälle bearbeiten  $\Rightarrow$  es wird Personal frei)

**Datenschutz:** Der Aufwand, der betrieben werden muss, um den Datenschutzrichtlinien gerecht zu werden.

**Ethik:** Die ethische Vertretbarkeit der Technologie. Hierunter fallen auch die 'Kosten' für die Gesellschaft, wenn die Technologie nicht verwendet wird.

**Politischer Wille:** Der politische Wille, dass die Technologie eingesetzt wird. Dazu gehört auch die „Authority to Execute“ also die Fähigkeit den Politischen Willen auch durchzusetzen. Hier sind hemmende Faktoren wie eine zu große Bürokratie wirksam.

Als weitere Bewertungsgrößen wurde noch Strafverfolgungschancen so wie technologischer Reifegrad verwendet. Diese können hier allerdings nicht voll gelistet werden.

## Transformationsfunktionen

Kröll listet in seiner Dissertation eine Vielzahl von Transformationsfunktionen auf. Da wir in unserer Arbeit aufgrund von Expertenmangel allerdings keine komplexen Merkmalverteilungen besitzen, bietet ein umfangreiches Eingehen auf alle diese Funktionen keinen Mehrwert. Wir beschränken uns also auf einige wenige Transformationsfunktionen, welche als ausreichend ausdrucksfähig für die Zwecke dieses Beitrags angesehen werden (siehe Tabelle 1)

Tabelle 1 Transformationsfunktionen

Transformationsfunktion	$x \in [-2,2]$	$x \in [1,5]$
steigend	$f(x) = \frac{x}{2}$	$f(x) = \frac{x-3}{2}$
fallend	$f(x) = -\frac{x}{2}$	$f(x) = \frac{3-x}{2}$



## Analysebeispiel: Kryptographie

Im Folgenden wird die Technologie Kryptographie bewertet und analysiert werden. Hierfür werden zuerst die Merkmalausprägung der drei Technologiegrößen „Kosten“, „Strafverfolgungspotenzial“ und „Reifegrad“ festgestellt. Dies wird dann gemäß obiger Erläuterung benutzt, um die Bewertungsverteilung zu berechnen und graphisch darzustellen. Zudem wird die TRN und eine Kartographierung der Technologie auf dem Hype-Cycle vorgenommen. Abschließend wird ein Zwischenfazit gegeben. Die Forschung im Feld der Kryptographie hat aktuell viele Schwerpunkte, wie die folgende Liste<sup>1</sup> zeigt. Eine Bewertung entsprechend der einzelnen Schwerpunkte und nicht dem Oberbegriff „Kryptographie“ würde einer fundierten Bewertung gerecht werden, überschreitet aber gleichzeitig den Rahmen des Machbaren für diesen Beitrag:

- Fingerprinting & Watermarking
- Hybrid & Asymmetric Key Encryption
- Security in Peer-to-peer Groups
- Threshold Cryptography & Multi-Party Multiplication
- Key Maintenance & Distribution
- Authentication & Prescribed Techniques
- Digital Forensics & Security
- Number Theories & Elliptic Curve Cryptography
- Traitor Tracing & Transmission Encryption
- Hashing & Block Ciphers
- Secrecy in E-Voting
- Database Security \ Privacy and Access Control

Beispielhaft gehen wir nun den Prozess der Bewertung nach Kröll [11] hier mit Kryptographie durch.

### Kosten

Die Kosten wurden in folgende Unterkategorien aufgeteilt. Die Merkmale werden von Experten bewertet und wurden hier als Machbarkeitsstudie von den Autoren vorgenommen.

---

<sup>1</sup> <https://phdservices.org/cryptography-topics-for-project/>

Merkm al	P	Begründung
Dauerhafte Kosten	1	Durch die Verwendung von Kryptographie werden klar dauerhafte Kosten entstehen. Hierunter fallen z. B. um Techniker, welche sich um die Implementierung der Technik kümmern und bei Problemen unterstützen. Weiter müssen gelegentlich Zertifikate (SSH) oder Lizenzen für Programme erworben werden. Da Kryptographie allerdings ein sehr standardisiertes und verbreitetes Verfahren ist, sind diese Kosten sehr gering.
Einmalige Kosten	1	Einmalig müssen Kosten für Techniker berechnet werden, welche z. B. standardmäßige Verschlüsselung von Emails oder Laufwerken einrichten. Weiter müssen gegebenenfalls Lizenzen für Programme erworben werden. Das gesamte Personal muss initial geschult werden und fällt somit kurzzeitig aus, wodurch Kosten entstehen. Im Vergleich zu anderen Technologien, fallen diese Kosten jedoch sehr gering aus.
Wartungs- kosten	0	Kryptographie ist bereits sehr weit verbreitet und standardisiert. Es ist davon auszugehen, dass nahezu keine Ausfälle während des Betriebs auftreten.
Kosten durch Fehl- anwen- dung	0	Sollte ein Angehöriger der Polizei die Möglichkeiten der Kryptographie falsch anwenden, sind im schlimmsten Fall, dass ein Schlüssel verloren geht und hierdurch Daten unwiderruflich verschlüsselt sind oder (persönliche) Daten von Unbefugten gelesen werden können. Dies ist nichts Neues, was durch versehentliches Löschen oder Verbreiten von Daten nicht auch schon geschieht.
Perso- nelle Kosten	1	Es müssen Techniker/Informatiker für die Implementierung und den Laufenden bereitgestellt werden. Es bedarf aber keiner neuen Abteilung oder Inspektion.
Schu- lungs- kosten	1	Initial müssen alle Angehörigen der Polizei auf z. B. Verschlüsselungen von Emails, Laufwerken und Ordnern geschult werden. Dies bedarf weniger Stunden und ist in jedem Fall nicht so umfangreich, wie die Implementierung eines neuen Fallbearbeitungsprogramm.
Mehr- auf- wand	1	Wird die Kryptographie bei der Polizei verwendet, müssen die Angehörigen der Polizei diese in ihrem Alltag verwenden. Auch wenn in vielen Szenarien dies automatisch ohne einen Mehraufwand des/der Angehörigen geschieht, ist in regelmäßigem Abstand mit einem geringen Mehraufwand zu rechnen.
Daten- schutz	2	Durch die Kryptographie wird der Datenschutz in besonderem Maße gefördert.

Ethik	2	Die Verschlüsselung von (persönlichen) Daten, die Signierung und der Wahrung von Integrität ist in jedem Fall ethisch vertretbar.
Politischer Wille	0	Nach aktuellen politischen Debatten ist 'der Politik' die Verwendung von Kryptographie egal.

Die Bewertung wird in P beschrieben und liegt im Intervall [-2,2].

### Strafverfolgungschancen

Die Bewertung wird in S beschrieben und liegt im Intervall [-2,2]. Für die Bewertung des Dual-Use in der Polizeiarbeit ist die Relevanz und damit der Einfluss auf die Bevölkerung ausschlaggebend. Die Aufspaltung der Merkmale sind hier Teil des wissenschaftlichen Diskurs und sollten kritisch diskutiert werden.

Merkmal	S	Begründung
Wirkung auf Bevölkerung	1	Die Bevölkerung wird die Verwendung der Kryptographie bei der Polizei eher befürworten, da hierdurch zum einen der Datenschutz erhöht werden kann, sich zum anderen aber auch neue Möglichkeiten zur Bürgeraufklärung ergeben können.
Zukunftsrelevanz Schlüsseltechnologie	1	Die Kryptographie ist bereits in den Alltag eines jeden Menschen in der digitalen Welt vorgedrungen, ob bewusst oder unbewusst. Aufgrund der immer weiter voranschreitenden Digitalisierung wird die Kryptographie zukünftig an Bedeutung gewinnen. Gleichzeitig sind Weiterentwicklungen in diesem Bereich zu erwarten.
Akzeptanz der Beamten	-1	Die Beamten folgen i.d.R., insbesondere mit steigendem Lebensalter, strikt dem Motto "alles bleibt so wie es ist" und stehen neuen Technologien grsl. ablehnend gegenüber. Wenn nun bei der Vorgangsbearbeitung neue Arbeitsschritte durch die Kryptographie hinzukommen, wird dies in weiten Teilen auf Ablehnung stoßen (vgl. Polyphone).
Komplett neue Delikte durch Kriminelle	1	So wie man Kryptographie verwenden kann, um seine eigenen Daten für andere unkenntlich zu machen, so können Kriminelle diese Technologie auch dazu verwenden, um die Daten anderer gegen deren Willen zu verschlüsseln.
Vereinfachung aktueller Delikte	2	Nahezu alle Kommunikationsmittel sind inzwischen verschlüsselt. Eine Auseinandersetzung mit Verschlüsselung und Kryptographie ist daher dringend notwendig, um die Kommunikation „klar“ für Ermittlungen vorliegen zu haben.

Schwerere Spuren- lage / Strafverfol- gung bei aktuellen Delikten	2	Sämtliche Aktionen im Internet oder generell auf Computern hinterlassen in irgendeiner Form Spuren, die gegebenenfalls ausgewertet werden können. Durch die Verwendung der Kryptographie werden auch diese Spuren in gewissem Maße verschlüsselt, was ein Auffinden beziehungsweise eine Auswertung dieser ohne den Schlüssel nahezu unmöglich macht.
Schadens- höhe durch neue De- likte	1	Durch die Kriminellen wird häufig ein Lösegeld erpresst, um die gegen den Willen der Opfer verschlüsselten Daten wieder zu entschlüsseln. Hierdurch entstehen insbesondere bei Unternehmen durch Produktionsausfälle hohe Schäden.
Schadens- höhe durch „alte“ De- likte	0	In Bezug auf „alte“ Delikte hat die Kryptographie nahezu keinen Einfluss.

### Reifegrad

Der Reifegrad einer Technologie hilft bei der Einschätzung der weiteren Entwicklung. Eine Ausgereifte Technologie hatte mehr Zeit Ansätze für Missbrauch zu verhindern. Hier ist die Bewertung R im Intervall [1,5].

Merkmal	R	Begründung
Ausgereift- heit Tech- nologie	4	Die Kryptographie ist schon weit verbreitet und technisch gut ausgereift. Dennoch ist in einigen Bereichen, insbesondere beim Schlüsselmanagement Verbesserungsbedarf.
Erklärbar- keit	5	Die Kryptographie folgt numerischen Grundsätzen und ist anhand einiger Vereinfachung leicht erklärbar.
Kompeten- zen	2	Grundsätzlich ist jeder bei der Polizei in der Lage einen Computer mit entsprechenden Programmen zu bedienen. Jedoch stellt die Einführung neuer Programme immer wieder eine Herausforderung dar. Zum einen Seitens der User (mangelnde Kompetenz), zum anderen Seitens der IT (mangelndes Personal).
Weiterent- wick- lungspo- tential	3	Die Basis der Kryptographie ist bereits solide. Jedoch gibt es weiterhin Möglichkeiten die Verschlüsselungen noch sicherer zu machen oder das Schlüsselmanagement (insbesondere bei der behördenübergreifenden Kommunikation) zu vereinfachen.

Anwendungs- breite	2	Die Anwendung der Kryptographie beschränkt sich darauf, die Daten zu verschlüsseln und den Datenaustausch zu sichern. Daher ist die Anwendungsbreite als eher schmal zu beurteilen.
Gerichts- festigkeit	2	Durch die Anwendung der Kryptographie werden keine Daten verändert. Somit ist keine gerichtliche Beanstandung zu erwarten. Vielmehr nutzt die Justiz selbst Verschlüsselungen (EGVP).
Justizielle Akzeptanz	2	Die Justiz verwendet eine eigene Verschlüsselung (EGVP). Somit müssten die Kompetenzen vorhanden sein, die von der Polizei genutzte Verschlüsselung ebenfalls anwenden zu können.
Dauer der Implementierung	2	Die Kryptographie an sich ist sofort verfügbar. Jedoch bedarf diese eine Anpassung auf die Bedürfnisse der Polizei. Weiterhin müssen alle Geräte mit den entsprechenden Programmen ausgestattet und alle Beamten geschult werden.

### Analysebeispiel: Virtual Reality

Als weiteres Beispiel für die Bewertung einer Technologie, widmen wir diesem Kapitel der „Virtual Reality“. Weniger soll es hierbei um die präzise Bewertung dieser gehen als um das Veranschaulichen der oben angesprochenen Punkte: Dies umfasst erstens die Möglichkeit, nachzuvollziehen, dass sich das ausgearbeitete Bewertungsschema problemlos auf eine weitere Technologie, und nicht nur die Kryptographie, anwenden lässt sowie zweitens dem Veranschaulichen des Gegenüberstellens zweier bewerteter Technologien.

### Schlussfolgerung

Ziel dieser Publikation ist es, ein mögliches Bewertungsschema für Technologien vorzustellen, welches im öffentlichen Dienst bei der Polizei eingesetzt werden könnte, um mögliche Inhalte für die Entwicklung von Curricular für ein Studium auszuwählen. Als Teil eines Technologieradars auch für die Bewertung zukünftiger Technologien und deren Dual-Use Potentials [10]. Hierzu haben wir das Bewertungsschema nach Kröll sowie den Hype-Cycle am Beispiel der Kryptographie und der Virtual Reality genutzt. Durch diese zwei exemplarischen Bewertungen konnten klar die Stärken dieses Bewertungsschemas aufgezeigt werden, da auf einen Blick mittels der visuellen Darstellung der Technologiegrößenbewertungsverteilung ersichtlich ist, dass hier die Kryptographie eine vielversprechendere Technologie ist als die Virtual Reality.

## Referenzen

- [1] Serkan Altuntas, Turkey Dereli, and Andrew Kusiak. Forecasting technology success based on patent data. *Technological Forecasting and Social Change*, 96:202–214, 2015.
- [2] H. Igor Ansoff. *Strategies for Diversification*. Harvard business review, 1957.
- [3] David Banta. What is technology assessment? *International journal of technology assessment in health care*, 25(S1):7–9, 2009.
- [4] Yonghee Cho and Tugrul Daim. Technology forecasting methods. In *Research and technology management in the electricity industry: Methods, tools and case studies*, pages 67–112. Springer, 2013.
- [5] Norman Dalkey and Olaf Helmer. An experimental application of the delphi method to the use of experts. *Management Science*, 9(3):458–467, 1963.
- [6] Eirma. *Technology roadmapping - delivering business vision*. Working group report, European Industrial Research Management Association, Paris, 1997.
- [7] Johannes Fähndrich, Ing Jürgen Beyerer, and Dipl-Math Jennifer Sander. *Analyse von Verfahren zur Kombination von Expertenwissen in Form von Wahrscheinlichkeitsverteilungen im Hinblick auf die verteilte lokale Bayes' sche Fusion*. PhD thesis, Diploma thesis, Karlsruhe Institut of Technology (May 2010), 2010.
- [8] John Forge. A note on the definition of “dual use”. *Science and Engineering Ethics*, 16:111–118, 2010.
- [9] A Henne. *Nutzwertanalyse*. In *Operational forest management planning methods: proceedings, meeting of steering systems project group*, International Union of Forestry Research Organizations, Bucharest, Romania, June 18-24, 1978. Navon, Daniel, Compiler.
- [10] Wilfried Honekamp, Roman Povalej, Heiko Rittelmeier, Johannes Fähndrich, Silvio Berner, and Dirk Labudde. *Technologiegetriebene polizeiausbildung im umgang mit digitalen spuren*. unknown, 2023.
- [11] Markus Kröll. *Methode zur Technologiebewertung für eine ergebnisorientierte Produktentwicklung*. PhD thesis, Universität Stuttgart, 2007.
- [12] A. Linden and J. Fenn. *Understanding gartner's hype cycles*. Strategic Analysis Report No. R-20-1971. Gartner Inc, 2003.
- [13] Joseph P Martino. A review of selected recent advances in technological forecasting. *Technological forecasting and social change*, 70(8):719–733, 2003.
- [14] Seumas Miller and Michael J Selgelid. Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. *Science and engineering ethics*, 13:523–580, 2007.
- [15] Jordi Molas-Gallart. Which way to go? defence technology and the diversity of 'dual-use' technology transfer. *Research policy*, 26(3):367–385, 1997.
- [16] Päivi Parviainen, Maarit Tihinen, Jukka Kääriäinen, and Susanna Teppola. *Tackling the digitalization challenge: how to benefit from digitalization in*

practice. *International journal of information systems and project management*, 5(1):63–77, 2017.

[17] Pfeiffer and Dögl. *Technologie-Portfolio-Management*. unknown, 1986.

[18] Robert Phaal, Clare JP Farrukh, and David R Probert. Characterisation of technology road-maps: purpose and format. In *PICMET'01. Portland International Conference on Management of Engineering and Technology. Proceedings Vol. 1: Book of Summaries (IEEE Cat. No.01CH37199)*, pages 367–374. IEEE, 2001.

[19] Günther Schuh. *Innovationsmanagement*. Springer Berlin, Heidelberg, 2012.

[20] Dieter Specht and Stefan Behrens. Strategische planung mit roadmaps — möglichkeiten für das innovationsmanagement und die personalbedarfsplanung. In *Technologie-Roadmapping*, pages 141–160. Springer-Verlag, unknown.

[21] John Vieyra, Mark Scanlon, and Nhien-An Le-Khac. Solid state drive forensics: Where do we stand? In *Digital Forensics and Cyber Crime: 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10–12, 2018, Proceedings 10*, pages 149–164. Springer, 2019.

[22] Horst Wildemann. *Strategische Investitionsplanung*. Gabler Verlag, 1987.

[23] Maria A. Wimmer, Gabriela Viale Pereira, Alexander Ronzhyn, and Vera Spitzer. Transforming government by leveraging disruptive technologies: Identification of research and training needs. *JeDEM - eJournal of eDemocracy and Open Government*, 12(1):87–113, Jul. 2020.

[24] Johan G Wissema. Trends in technology forecasting. *R&D Management*, 12(1):27–36, 1982.

[25] David Wright. A framework for the ethical impact assessment of information technology. *Ethics and information technology*, 13:199–226, 2011.

[26] Stephan Zollner, Kim-Kwang Raymond Choo, and Nhien-An Le-Khac. An automated live forensic and postmortem analysis tool for bitcoin on windows systems. *IEEE Access*, 7:158250–158263, 2019.