BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Projekt Cybercrime (Ausgabenbewilligung; Änderung des Dekrets zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (Dekret EG StPO); Beantwortung Postulat 2017/186 «Kantonale Strategie Cyber-Kriminalität»)

2017/186

vom 25. Juni 2019

1. Übersicht

1.1. Zusammenfassung

Delikte im Bereich Cybercrime nehmen stetig zu. Diese Tendenz wird sich auch in Zukunft nicht verändern. Die Cyberkriminalität betrifft aufgrund der zunehmenden Digitalisierung der Gesellschaft zahlreiche Lebensbereiche und fast die gesamte Bevölkerung. Der volkswirtschaftliche Schaden, der durch Cyberkriminalität verursacht wird, ist sehr gross. Die Bevölkerung erwartet von den Strafverfolgungsbehörden, dass diese Delikte verfolgt und geahndet werden.

Demgegenüber stehen die aktuellen Handlungsmöglichkeiten der Strafverfolgungsbehörden des Kantons Basel-Landschaft (Staatsanwaltschaft und Polizei Basel-Landschaft) bei der Bekämpfung der Cyberkriminalität. Aufgrund der personellen und finanziellen Ressourcen sowie aufgrund des vorhandenen Fachwissens ist es zurzeit nicht möglich, Delikte aus dem Bereich Cybercrime in der geforderten Qualität und Quantität zu bekämpfen.

Angestossen durch die aktuelle Situation im Bereich Cybercrime und durch das Postulat: 2017/186: «Kantonale Strategie Cyber-Kriminalität» wurde das Projekt Cybercrime lanciert. Das von der Staatsanwaltschaft und der Polizei Basel-Landschaft gemeinsam geführte Projekt hat das Ziel, eine Strategie zur Bekämpfung der Cyberkriminalität im Kanton Basel-Landschaft zu erstellen. Diese Strategie liegt nun vor.

Die Strategie basiert auf vier Pfeilern. Es sind dies: Aus- und Weiterbildung, Spezialisierung, Prävention und Repression. Währendem das Thema Prävention praktisch ausschliesslich eine Aufgabe der Polizei ist, betreffen die drei anderen Themen sowohl die Staatsanwaltschaft als auch die Polizei Basel-Landschaft gleichermassen und haben Auswirkungen auf beide Organisationen.

Die organisatorischen Auswirkungen der Umsetzung der Strategie sind die Folgenden:
Die Staatsanwaltschaft schafft einen Fachbereich Cybercrime, dessen Schwerpunkt die Untersuchung und Anklage in definierten Fällen von Cybercrime ist. Dieser Fachbereich wird der Hauptabteilung Betäubungsmittelkriminalität und organisierte Kriminalität angegliedert.
Die Polizei Basel-Landschaft schafft eine Abteilung Cybercrime, bestehend aus den Fachbereichen IT-Forensik, IT-Ermittlung und IT-Überwachung, die in die Hauptabteilung Kriminalpolizei eingegliedert wird.
Ziel dieser Einbettungen ist es, das Know-how im Bereich Cybercrime zu konzentrieren und eine effiziente Arbeitsweise zu ermöglichen mit klar definierten Zuständigkeiten und Ansprechpersonen.

Die Umsetzung der Strategie hat die folgenden Auswirkungen in personeller und finanzieller Hinsicht:
Bei der Staatsanwaltschaft sind zwei zusätzliche Staatsanwälte oder Staatsanwältinnen sowie ein Untersuchungsbeauftragter oder eine Untersuchungsbeauftragte erforderlich.
Bei der Polizei Basel-Landschaft sind 13 neue Stellen notwendig.
Die Schaffung der neuen Stellen haben eine jährlich wiederkehrende Ausgabe von CHF 2'100'589.00 zur Folge. Im Weiteren fallen zusätzlich wiederkehrende Folgekosten von jährlich CHF 849'000.00 und einmalige Folgekosten von CHF 3'142'500.00 an. Die Ausgabe des Betrages von jährlich CHF 2'100'589.00 für die zusätzlichen Stellen ist durch den Landrat zu bewilligen. Für die Umsetzung der Einführung der beiden zusätzlichen Stellen einer Staatsanwältin oder eines Staatsanwaltes ist die Anpassung des Dekrets zum Einführungsgesetz zur Schweizerischen Strafprozessordnung durch den Landrat erforderlich.

Die Umsetzung der Strategie erfolgt schrittweise über einen Zeitraum von vier Jahren ab Beschluss des Landrates.

1.2. Inhaltsverzeichnis

2. Bericht

2.1. Ausgangslage

2.1.1. Postulat: 2017/186: «Kantonale Strategie Cyber-Kriminalität»

Am 18. Mai 2017 reichte Landrat Klaus Kirchmayr ein Postulat zum Thema «Kantonale Strategie Cyber-Kriminalität» ein[1]. Mit dem Postulat wird beantragt, dass der Regierungsrat beauftragt wird, «eine langfristige Strategie zur Bekämpfung der Cyber-Kriminalität inklusive der notwendigen Massnahmen bezüglich Mitteln, Mitarbeitern und Strukturen zu entwickeln. Diese Massnahmen sollen mittelfristig in den Aufgaben- und Finanzplan des Kantons einfliessen können. Dem Landrat ist in Form eines Strategiepapiers Bericht zu erstatten.»

Begründet wurde das Postulat wie folgt:
«Die Digitalisierung macht auch vor den dunklen Seiten unserer Gesellschaft keinen Halt. Der Anteil der Cyber-Kriminalität an der Gesamt-Kriminalität ist stetig im Steigen begriffen und alle Experten sind sich darin einig, dass sich diese Entwicklung weiter beschleunigen wird. Vom Identitäts-Diebstahl, Internet-Betrug, Internet-Mobbing, Stalking bis hin zum qualifizierten Bankeinbruch reicht die Palette der Delikte. Da sich Daten und Netzwerke zudem kaum um Grenzen oder sonstige Regeln kümmern, ergeben sich für die Verfolgung entsprechender Cyber-Delikte grosse neue Herausforderungen.
Auch wenn die Strafverfolgungsbehörden in Bezug auf die Digitalisierung Fortschritt gemacht haben, so sind sie in ihrem Kern bezüglich Organisation, ihrer Abläufe, der Ausbildung ihrer Mitarbeiter und Mittel im Wesentlichen noch immer „analog" unterwegs.

Eigentlich kommt dem Bund bei der Bekämpfung der Cyber-Kriminalität eine zentrale Rolle zu. Doch der Zustand der diesbezüglichen Stellen in Bern kann in keinster Weise befriedigen. Eine hohe Fluktuation, eine sehr schlechte Ressourcierung und fehlende Mittel und Skills an allen Ecken und Enden kennzeichnen die Situation.

Verschiedene Kantone haben deshalb reagiert und ihre eigenen Kapazitäten in diesem Bereich gebündelt und aufgestockt. Die Kantone Bern und Zürich sind hier zu nennen. Der Kanton Zürich hat ein eigenes Cyber-Kriminalitätszentrum geschaffen wo über 30 Profis aus Polizei und Staatsanwaltschaft diese Thematik gebündelt angehen. Angesichts der Schäden, welche Internetkriminalität anrichtet ist dies nicht nur eine Notwendigkeit, sondern auch eine sich mehr als auszahlende Investition in den Wirtschaftsstandort Zürich mit seinem Anspruch ein führender IT-Wirtschaftsstandort zu werden.

Die gleichen Herausforderungen, wie sie sich in Zürich und Bern stellen finden sich auch bei uns.»

Das Postulat wurde mit 62:11 Stimmen an den Regierungsrat überwiesen.

[1] Parlamentarischer Vorstoss 2017/186

2.1.2. Definition Cyberkriminalität

Terminologisch wird im Folgenden zwischen «Cyberkriminalität im engeren Sinn» (Cybercrime ieS) und «Digitalisierter Kriminalität» (DigiKrim) unterschieden. Mit Cybercrime ieS sind Straftaten gegen das Internet und seine Instrumente, mit DigiKrim (auch: «Cyberkriminalität im weiteren Sinn») «klassische» Delikte, die unter Zuhilfenahme von Mitteln der Internettechnologie verübt werden, gemeint. «Cyberkriminalität», «Cybercrime» und «Computerkriminalität» meinen im Folgenden alle das Gleiche und dienen als übergeordnete Begriffe über «Cybercrime ieS» und «DigiKrim».

Die Phänomene, die im Zusammenhang mit Cyberkriminalität in Erscheinung treten, sind zahlreich. Beispiele dafür sind: Phishing, Eindringen in Datenverarbeitungsanlagen, Account Hijacking, Skimming, falsche Überweisungsaufträge, betrügerische Angebote, Bestellungsbetrug, verbotene Pornographie und viele mehr. Wenn in der Vorlage von Cybercrime gesprochen wird, sind damit immer beide Bereiche gemeint, also Cybercrime ieS und DigiKrim.

2.1.3. Allgemeines zum Thema Cyberkriminalität / Auswirkung der Digitalisierung

«Der Cyber-Bereich ist hoch dynamisch und was gestern noch als state-of-the-art galt, ist heute bereits kalter Kaffee.»[2] So sind im – durch raschen Wandel gekennzeichneten – Cyber-Bereich eine zunehmende Professionalisierung der Täterschaft, eine kontinuierliche Verfeinerung bereits bekannter und erprobter «modi operandi», aber auch eine stete Entwicklung neuer Tathandlungen festzustellen. Darüber hinaus existieren gerade im Cyber-Bereich keine Landesgrenzen. So kommt es beispielsweise vor, dass sich situativ mehrere Täter, die sich zwar online, nicht aber persönlich kennen, zusammenschliessen, um gemeinsam einen transnationalen Angriff durchzuführen. Ferner ist gerade Cybercrime ieS komplex. Allerdings ist festzustellen, dass auch im Bereich der digitalisierten und herkömmlichen Kriminalität vermehrt Anonymisierungsdienste sowie – mittlerweile zunehmend verschlüsselte – Mittel der Informations- und Kommunikationstechnik eingesetzt werden. Eine effektive und effiziente Reaktion auf Cybercrime-Vorfälle setzt deshalb ein zeitnahes, zielgerichtetes und koordiniertes Vorgehen aller Beteiligten (Direktbetroffene, kantonale Strafverfolgungsbehörden, Bundesbehörden, internationale Behörden und Akteure, etc.) voraus.

Die Komplexität bei der Sicherung, Aufbereitung, Auswertung und Dokumentation von gesicherten digitalen Datenbeständen und der daraus resultierenden Fragestellungen nimmt je länger je mehr zu. Die Datenvolumina steigen stetig, und dies im gesamten Kriminalitätsbereich, nicht nur im Bereich Cybercrime. Der damit verbundene Aufwand im Zusammenhang mit der Beweiserhebung und Beweissicherung nimmt laufend stark zu. Ebenso die Anforderungen an das technische Know-how. Zudem kommen mit den Bereichen Fahrzeug- und IoT-Forensik[3] komplexe neue Aufgabenfelder hinzu und die Cloud, bzw. ihre Möglichkeiten, nehmen im Geschäfts- wie auch im Privatbereich einen immer grösseren Stellenwert ein.

Im Bereich der verdeckten Überwachungsmassnahmen ist seit mehreren Jahren eine markante Zunahme des zu betreibenden Aufwands feststellbar, zumal klassische Ermittlungsmassnahmen immer weniger greifen. IT-Fachwissen ist in diesem Bereich künftig unabdingbar, um die Sachbearbeitenden zu unterstützen.

[2] MELANI, 1. Halbjahresbericht 2017 (Januar-Juni), Seite 73 i.f. (https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-1.html (abgerufen am 13.02.2019)

[3] Internet of Thing, Internet der Dinge, beispielsweise smarte Lautsprecher etc.

2.1.4. Entwicklung der Fallzahlen im Bereich der Cyberkriminalität im Kanton Basel-Landschaft

Von 2015 bis 2018 wurde bei der Polizei Basel-Landschaft ein Anstieg bei den Fallzahlen von 270 auf 471 registriert.

	2015	2016	2017	2018
Cybercrime ieS	74	75	111	100
DigiKrim	196	256	280	371
Total	**270**	**331**	**391**	**471**

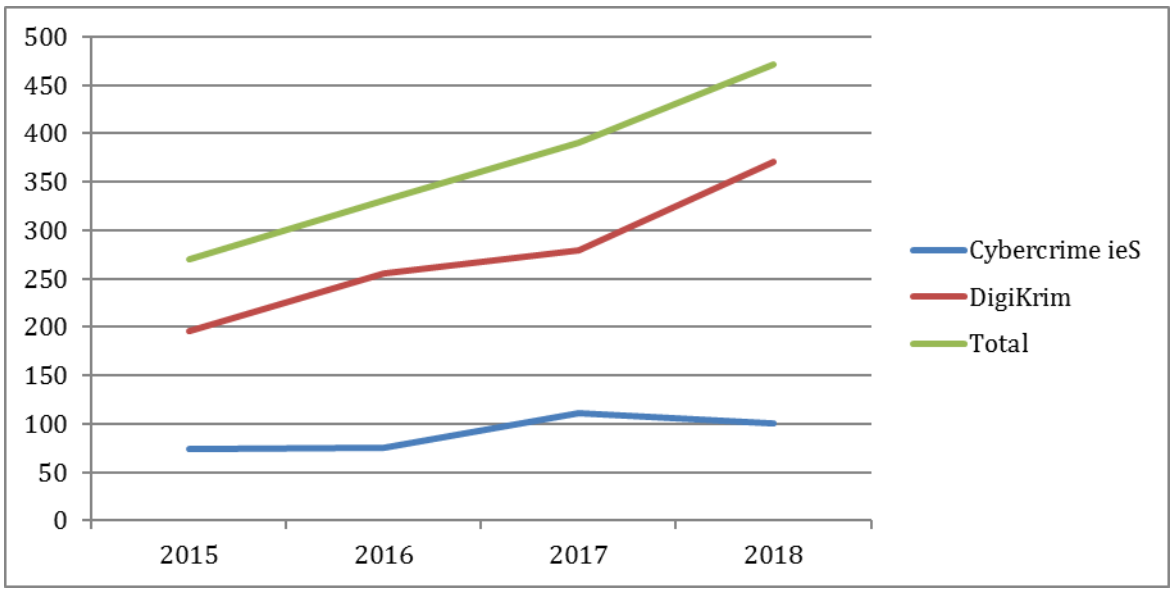

Abb. 1: Fallzahlenanstieg von 2015-2018

Der in den vergangenen Jahren im Kanton Basel-Landschaft zu beobachtende Anstieg der jährlichen Fallzahlen von durchschnittlich 20% korrespondiert mit den langjährigen Beobachtungen des Kompetenzzentrums Cybercrime der Staatsanwaltschaft Zürich, welches eine jährliche Zunahme der Cybercrime-Fälle um jeweils 10 bis 30 % verzeichnet.

Es ist davon auszugehen, dass der beobachtete Anstieg der Fallzahlen auch in den folgenden Jahren weiter bestehen bleibt.

Im Zusammenhang mit den erhobenen Fallzahlen ist zudem zu erwähnen, dass im Bereich Cyberkriminalität gemeinhin von einer sehr hohen Dunkelziffer ausgegangen wird. Fachleute (vorwiegend aus Deutschland) gehen von einer Dunkelziffer von 75 bis 90 % aus.

2.1.5. Volkswirtschaftlicher Schaden verursacht durch Cybercrime

Der durch Cyberkriminalität verursachte Schaden ist sehr hoch. Konkrete Schadenssummen lassen sich nicht erheben. Für Deutschland wird der Schaden auf mehrere Milliarden Euro geschätzt. Der Schweizerische Versicherungsverband schätzt in einem Grundlagenpapier die jährlichen Kos-

ten für Cyber-Risiken in der Schweiz auf bis zu 9,5 Milliarden Schweizer Franken, Tendenz steigend.[4]

2.1.6. Entwicklungen der Bekämpfung Cybercrime auf nationaler Ebene

Anfang 2018 wurde die «Strategie zur effizienten Bekämpfung von Cybercrime» durch die Bundesanwaltschaft, das Bundesamt für Polizei, die Konferenz der kantonalen Polizeikommandanten der Schweiz und die Schweizerische Staatsanwälte-Konferenz verabschiedet. Ziel dieser Strategie ist es, mittels Koordination zwischen den Kantonen und dem Bund sicherzustellen, dass es im Cyberspace keine rechtsfreien Räume gibt.

Cyberboard
Das Cyberboard[5] ist eine Koordinationsplattform und wurde ausgehend vom Gedanken, wonach die Bekämpfung der Cyberkriminalität eine Verbundsaufgabe von kantonalen und nationalen Behörden auf Ebene Polizei und Staatsanwaltschaft ist, ins Leben gerufen.

Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK)
NEDIK, als Bestandteil des Cyberboards, soll den Wissenstransfer zwischen den kantonalen Polizeikorps sowie zwischen den Bundesbehörden und kantonalen Polizeikorps sicherstellen.

Melde- und Analysestelle Informationssicherung (MELANI)
Bei MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.[6]

Die vorerwähnten Institutionen sind ein Teil der Massnahmen im Bereich der Strafverfolgung in der vom Bundesrat verabschiedeten Nationalen Cyberstrategie 2018-2022 (NCS)[7,8].

Bund
Der Bundesrat hat am 30. Januar 2019 die Aufgaben und Zuständigkeiten im Bereich Cyber-Risiken festgelegt und einen Cyber-Ausschuss ins Leben gerufen. Ein neu zu schaffendes Kompetenzzentrum soll möglichst rasch seine Tätigkeit als nationale Anlaufstelle für Fragen zu Cyber-Risiken aufnehmen. Die strategische Leitung übernimmt eine Delegierte oder ein Delegierter für Cyberfragen.[9]
Der Bundesrat hat an seiner Sitzung vom 15. Mai 2019 einen Entscheid zum Aufbau des Kompetenzzentrums Cyber-Sicherheit gefällt und eine Stärkung der personellen Ressourcen im Bereich Cyber-Risiken im Umfang von 24 Stellen beschlossen. Diese Personalaufstockung wird nicht im Bereich der Strafverfolgung, sondern für die Bereiche Cyber-Sicherheit und Cyber-Risiken erfolgen. Damit wird es zu keiner Entlastung der Kantone im Bereich der Strafverfolgung kommen.

2.1.7. Entwicklung der Bekämpfung Cybercrime in den einzelnen Kantonen (Stand Januar 2019)

Die Zuständigkeit der einzelnen Kantone in der Bekämpfung von DigiKrim und Cybercrime ieS (vgl. nachfolgend «Rechtliche Grundlagen zur Verfolgung der Cyberkriminalität durch die kantonale Staatsanwaltschaft») hat dazu geführt, dass in den Kantonen entsprechende Prozesse definiert wurden oder Projekte angelaufen oder geplant sind.

---

[4] Grundlagenpapier Schweizerischer Versicherungsverband zu Cyber-Risiken vom 22.02.2018 (https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf, abgerufen am 20.02.2019)
[5] Koordinationsgremium für die Analyse der Ausgangslage und Bearbeitung von Cybercrime-Meldungen. Das Cyberboard verfügt neben dem strategischen Organ (Cyber-STRAT) über einen operativen Bereich (Cyber-CORE), welcher in die Teilbereiche Cyber-CASE) und Cyber-STATE unterteilt ist. Dem Cyber-STRAT gehören unter anderem die Schweizerische Staatsanwälte-Konferenz (SSK), die Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS), die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), die Bundesanwaltschaft (BA) und das Bundesamt für Polizei (fedpol) an.
[6] Website MELANI https://www.melani.admin.ch/melani/de/home.html (abgerufen am 06.03.19)
[7] https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (abgerufen am 30.01.2019)
[8] Zu diesem Thema vgl. auch https://www.vbs.admin.ch/de/verteidigung/schutz-vor-cyber-angriffen.html (abgerufen am 13.02.19)
[9] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73839.html (abgerufen am 13.02.2019)

Im Polizeikonkordat Nordwestschweiz (PKNW) hat die Kantonspolizei Bern als Vorreiterin eine Kerngruppe Cybercrime, bestehend aus Elementen der Ermittlung, Forensik, Innenfahndung und Prävention aufgestellt, um die verschiedenen Fachbereiche und Kompetenzen in Bezug auf die Fallbearbeitung eng zusammenarbeiten zu lassen. Die Staatsanwaltschaft Basel-Stadt, die Polizei Solothurn und die Kantonspolizei Aargau sind zurzeit in ähnlichen Projekten und Änderungsprozessen. So hat die Kantonspolizei Aargau eine Ausschreibung für den Leiter einer Cybercrime-Abteilung geschaltet. Diese Person wird nach ihrer Wahl und dem Dienstantritt die Aufgabe übernehmen, Strukturen zur Bekämpfung von DigiKrim und Cybercrime ieS als Projekt an die Hand zu nehmen und umzusetzen. Bei der Polizei Solothurn und der Staatsanwaltschaft Basel-Stadt mit der dazugehörigen Kriminalpolizei sind Bestrebungen zur Schaffung von neuen Stellen im Gange, um die Organisationen in der Bekämpfung von Cybercrime fit für die Zukunft zu machen.

Ausserhalb des PKNW ist nebst dem Cybercrime Competence Center in Zürich die Kantonspolizei St. Gallen hervorzuheben.

2.1.8. Rechtliche Grundlagen zur Verfolgung der Cyberkriminalität durch die kantonale Staatsanwaltschaft

Die Schweizerische Strafprozessordnung (StPO) sieht vor, dass die kantonalen Strafbehörden zur Verfolgung und Beurteilung aller Straftaten des Bundesrechts zuständig sind, soweit keine gesetzlichen Ausnahmen vorliegen (Art. 22 StPO). Damit besteht bei der schweizerischen Strafverfolgung eine originäre kantonale Gerichtsbarkeit.[10]

Die gesetzlichen Ausnahmen der kantonalen Zuständigkeit finden sich in Art. 23 StPO unter dem Titel „Bundesgerichtsbarkeit im Allgemeinen“. Demnach ist grundsätzlich von einer Bundesgerichtsbarkeit auszugehen, wenn die Interessen des Bundes betroffen sind. Sodann ist gemäss Art. 23 Abs.1 StPO namentlich eine Bundeszuständigkeit in Strafsachen vorgesehen, wenn sich eine Straftat einer gewissen Schwere gegen Behördenmitglieder des Bundes richtet (lit. a) oder völkerrechtlich geschützte Räumlichkeiten und Gegenstände durch die Straftat bedroht sind (lit. b). Weiter übernimmt der Bund die Zuständigkeit bei gemeingefährlichen Straftaten, wie beispielsweise der Gefährdung durch Sprengstoffe und giftige Gase (lit. d; Art. 224 StGB) und der Zuständigkeit hinsichtlich Delikten der Geld- und Wertzeichen (lit. e; Art. 240 - 250 StGB). Daneben werden auch die Delikte zur Störung der Beziehungen zum Ausland durch die Bundesbehörden verfolgt (lit. i; Art. 296 - 302 StGB). Im Speziellen ist bei organisiertem Verbrechen, Finanzierung des Terrorismus und Wirtschaftskriminalität unter bestimmten Voraussetzungen eine Bundesgerichtsbarkeit vorgesehen (Art. 24 StPO). Ausserdem gibt es viele Bundesgesetze, welche direkt eine Bundesgerichtsbarkeit vorsehen, so zum Beispiel das Parlamentsgesetz, das Kriegsmaterialgesetz und das Kernenergiegesetz. Ungeachtet der Tatsache, dass in spezifischen Bereichen eine Bundeszuständigkeit vorgesehen ist, hat die Bundesanwaltschaft jedoch die Möglichkeit, die Untersuchung und Beurteilung von Strafsachen in Bundeskompetenz an die Kantone zu delegieren (Art. 25 StPO), womit eine Straftat selbst bei einer expliziten Bundeszuständigkeit durch die kantonalen Strafverfolgungsbehörden zu verfolgen und beurteilen ist.

Hinsichtlich der Cyberkriminalität lässt sich in der Schweizerischen Strafprozessordnung sowie in den Gesetzen des Nebenstrafrechts kein spezifischer Hinweis auf eine Bundesgerichtsbarkeit finden. Grundsätzlich richtet sich die Verfolgung der Cyberkriminalität darum nach der originären kantonalen Gerichtsbarkeit, wobei hier keine Unterscheidung zwischen DigiKrim und Cybercrime ieS besteht. Dies obwohl gerade im Bereich der Cyberkriminalität die Bezüge zum Ausland im Vergleich zu anderen Deliktsbereichen sehr häufig und ausgeprägt sind. Darum müssen selbst gros-

[10] BSK StPO, DANIEL KIPFER, Art. 22, N 2.

se, komplexe und international verstrickte Cybercrime-Fälle grundsätzlich durch die kantonalen Staatsanwaltschaften verfolgt werden.[11]

2.1.9. Möglichkeiten und Grenzen der Zusammenarbeit (national und interkantonal)

Die aktuellste Aufstockung des Bundes betreffend den Aufbau des Kompetenzzentrums Cyber-Sicherheit hat keinen Einfluss auf den Ressourcenbedarf der Strafverfolgungsbehörden des Kantons Basel-Landschaft. Die StPO definiert die Kompetenzverteilung zwischen Bund und Kantonen klar, was bedeutet, dass der Bund respektive die Bundesanwaltschaft nur ganz spezifische Verfahren übernimmt. Im Bereich Cyberkriminalität gibt es allerdings bis auf eine Ausnahme (Phishing-Fälle) keine Bundeszuständigkeit (Verweis auf Kap. 2.1.8). Interkantonale Kompetenzzentren wurden in verschiedenen Kantonen angedacht, sind jedoch zwischenzeitlich bereits wieder verworfen worden. Auch die Möglichkeit, Leistungen im Bereich der Strafverfolgung von Cyberkriminalität in anderen Kantonen einzukaufen, besteht aktuell nicht, da die Kantone, welche bereits ein Kompetenzzentrum errichtet haben (Kanton Zürich, Genf und St. Gallen), nicht über freie Ressourcen verfügen, um Dienstleistungen für Strafverfahren im Kanton Basel-Landschaft anzubieten. Es zeigt sich aktuell die Situation, dass nicht nur Basel-Landschaft, sondern auch weitere Kantone bestrebt sind ihre personellen und materiellen Ressourcen auf- respektive auszubauen, um ihre eigenen Strafverfahren im Bereich DigiKrim und Cybercrime ieS. zu bewältigen. Darüber hinaus ist zu berücksichtigen, dass bereits in den allermeisten Strafverfahren beziehungsweise bei den allermeisten Deliktsformen eine digitale Komponente vorhanden ist, welche immer mehr Ressourcen im Bereich in den beiden Strafverfolgungsbehörden, Polizei und Staatsanwaltschaft, erfordern. Einerseits hinsichtlich der Datenmenge anderseits betreffend die Datenkomplexität. Demzufolge ist eine Zusammenarbeit mit den anderen Kantonen respektive dem Bund auf den Fach- und Wissensaustausch beschränkt, welcher durch NEDIK und das CyberCase gewährleistet ist. Die Verantwortung zur Bearbeitung der einzelnen Verfahren bleibt somit in den einzelnen Kantonen, weshalb der Kanton Basel-Landschaft zwingend die eigenen Ressourcen zur Bewältigung dieser Thematik zur Verfügung stellen muss.

2.1.10. Bevölkerungsumfrage 2018

Die Polizei Basel-Landschaft liess im Jahr 2018 durch die Firma gfs-zürich eine repräsentative Bevölkerungsbefragung im Kanton Basel-Landschaft zur Wahrnehmung und Bewertung der Leistung der Polizei Basel-Landschaft durchführen[12]. Aus dieser Befragung können auch Aussagen zum Thema «Internetkriminalität» gemacht werden. So fürchten sich 28 % der Bevölkerung davor, Opfer von Internetkriminalität zu werden. In den letzten fünf Jahren wurde jeder zwölfte Einwohner Opfer von Internetkriminalität. Jedes fünfte Opfer von Internetkriminalität schaltete die Polizei ein. Nur die Hälfte der Opfer, die die Polizei einschaltete, war zufrieden mit den Leistungen der Polizei. Hingegen attestiert die Bevölkerung der Polizei grosse Fortschritte im Umgang mit Internetkriminalität.

Die Firma gfs-zürich kommt in der Auswertung der Umfrage zum Ergebnis, dass die Internetkriminalität im Jahr 2017 gegenüber den Vorjahren deutlich zugenommen hat. Fast die Hälfte der Personen, die in den letzten fünf Jahren (bis und mit 2017) Opfer von Internetkriminalität wurden, wurde dies im Jahre 2017. Die Opferrate hat sich in den letzten Jahren jeweils von Jahr zu Jahr fast

---

[11] Abweichend hiervon hat das Bundesstrafgericht bis dato einzig bei den sogenannten Phishing-Fällen (darunter werden täuschende Machenschaften verstanden, bei der die Täterschaft den Geschädigten mittels gefälschter Websites, E-Mails etc. dazu veranlasst, vertrauliche [Zugangs-]Daten [z.B. zum e-Banking] bekannt zu geben, um damit ein Vermögensdelikt zu begehen) eine Bundeszuständigkeit anerkannt. Dabei hat das Bundesstrafgericht die Bundeszuständigkeit allerdings auf die überwiegend im Ausland ansässigen Hintermänner beschränkt, während die Verfolgung der in der Schweiz tätigen Phishing-Finanzmanager in der Zuständigkeit der kantonalen Strafverfolgungsbehörden bleibt (Beschluss des Bundesstrafgerichts vom 27. November 2011, BG.2011.27). Die Übernahme weiterer Fälle von Cyberkriminalität durch die Bundesanwaltschaft ist nicht vorgesehen, auch wenn diese eine (interne) Liste mit Kriterien erarbeitet hat, welche beim Entscheid einer allfälligen Fallübernahme im Bereich Cybercrime herangezogen werden kann (Tätigkeitsbericht BA 2017, Ziff. 3).

[12] Repräsentative Bevölkerungsumfrage im Kanton Basel-Landschaft zur Wahrnehmung und Bewertung der Leistung der Polizei Basel-Landschaft, gfs-zürich, Juni 2018

verdoppelt. Zudem ist zu beobachten, dass nur 20 % der Opfer von Internetkriminalität die Polizei hinzugezogen hat.

Die Firma gfs-zürich kommt zum Schluss, dass die Internetkriminalität eine Herausforderung darstellt, welcher sich die Polizei Basel-Landschaft in Zukunft annehmen muss.

2.1.11. Projekt Cybercrime der Staatsanwaltschaft und der Polizei Basel-Landschaft

Am 21. September 2017 erstellten die Erste Staatsanwältin und der Polizeikommandant den Projekt-Initialisierungsauftrag Cybercrime. Mit der Ausführung des Auftrages wurde ein Projektteam, bestehend aus Mitarbeitenden der Polizei und der Staatsanwaltschaft, beauftragt.
Es wurden folgende Ziele definiert:

- Es existiert eine gemeinsame, mehrjährig gültige Strategie zur professionellen Reaktion auf die Cyberkriminalität. Diese Strategie basiert auf der Gesamtstrategie und Ausrichtung der Polizei Basel-Landschaft sowie derjenigen der Staatsanwaltschaft Basel-Landschaft und wird im Projekt Cybercrime umgesetzt.

- Es besteht ein Leistungskatalog Cybercrime mit entsprechenden Kriterien, welcher über konkrete Leistungen Auskunft gibt, die durch die Strafverfolgungsbehörden des Kantons Basel-Landschaft erbracht werden. Gleichzeitig ist definiert, welche Leistungen extern eingekauft werden müssen.

- Es besteht Klarheit über die rechtliche Zuständigkeit in der Anfangsphase von Untersuchungen.

- Es besteht Klarheit über den Aus- und Weiterbildungsbedarf bei Polizei und Staatsanwaltschaft Basel-Landschaft.

In der Folge verfasste das Projektteam die Projektstudie. Am 21. August 2018 wurde der Projektauftrag erteilt. Das Projekt befindet sich aktuell in der Konzeptphase.

2.1.12. Prüfung durch die Finanzkontrolle Basel-Landschaft

Die Finanzkontrolle des Kantons Basel-Landschaft prüfte das Projekt Cybercrime. Die Prüfung diente dazu festzustellen, welche strategischen und taktischen Massnahmen die Strafverfolgungsbehörden (Polizei und Staatsanwaltschaft) des Kantons Basel-Landschaft getroffen haben, um effektiv und effizient den Herausforderungen der Cyberkriminalität entgegenzutreten.

Die Finanzkontrolle stellte in ihrem Bericht vom 11.09.2018 fest, dass «derzeit für den Kanton Basel-Landschaft keine mittel- bis langfristige Strategie zur effektiven und effizienten Prävention, Abwehr und Bekämpfung von Straftaten im Bereich der Cyberkriminalität» existiert.[13] Sie stellte im weiteren fest, dass «die notwendigen Ressourcen (Personen, Sachmittel und Budget) für die Umsetzung einer Strategie nicht oder nicht im erforderlichen Umfang vorhanden»[14] sind. Im Rahmen der Kontrolle konnte die Finanzkontrolle Einsicht in den Entwurf der Projektstudie nehmen. Sie bewertet die Ergebnisse der Studie als sinnvoll und zielführend und empfiehlt die konsequente und zeitnahe Umsetzung.

2.1.13. Schlussfolgerung

Es ist unbestritten, dass die Fallzahlen im Bereich der Cyberkriminalität ansteigen. Mit der unablässig voranschreitenden Digitalisierung, die sich mittlerweile praktisch auf sämtliche Lebensbereiche erstreckt, wird diese Tendenz auch in den nächsten Jahren fortbestehen. Nicht nur die Kom-

[13]Bericht Nr. 024/2018 vom 11.08.2018 der Finanzkontrolle BL, S. 4
[14]Bericht Nr. 024/2018 vom 11.08.2018 der Finanzkontrolle BL, S. 4

plexität der Cyberkriminalität nimmt laufend zu, sondern auch die Digitalisierung in der gesamten Kriminalität. Diese Tendenz ist bereits seit Jahren festzustellen, da praktisch in jedem Verfahren digitale Daten vorhanden sind, deren Auswertung die Strafverfolgungsbehörden in starkem Masse belasten. Die heutigen Strukturen der Polizei Basel-Landschaft sowie der Staatsanwaltschaft reichen bereits heute nicht aus, dieser zunehmenden Digitalisierung im gesamten Kriminalitätsbereich effizient zu begegnen. Einerseits, weil oftmals die nötigen Personalressourcen fehlen, um die umfangsreichen Datenmengen innert nützlicher Frist auszuwerten, aber auch, weil die zur Verfügung stehende Soft- und Hardware sowie das Know-how nicht immer ausreichen, um die sichergestellten Datenträger der unterschiedlichsten Art auszuwerten. Mit den zu erwartenden steigenden Fallzahlen im Bereich Cybercrime, wird sich diese Situation weiter verschärfen. Es geht somit vorliegend nicht nur darum, den spezialisierten Bereich von Cybercrime ieS effizient bekämpfen zu können, sondern ganz allgemein darum, dass sich die Strafverfolgungsbehörden derart organisieren, dass der gesamten digitalen Entwicklung im Kriminalitätsbereich adäquat begegnet werden kann. Zudem verändern sich die Formen von DigiKrim und Cybercrime ieS laufend und erfordern Organisationsstrukturen, die eine angemessene Reaktion auf diese Veränderungen ermöglichen. Die Bekämpfung der DigiKrim und Cybercrime ieS, wie auch ganz allgemein der Umgang mit digitalen Komponenten in einem Strafverfahren, setzen zudem bei den Strafverfolgungsbehörden spezifische Kenntnisse und das Vorhandensein von speziellen Infrastrukturen voraus.

Es besteht unter anderem das Ziel, dass die Strafverfolgungsbehörden von der Bevölkerung als kompetente Stelle für die Bekämpfung der Cyberkriminalität wahrgenommen werden. Die Bekämpfung der Cyberkriminalität ist jedoch zeit-, personal- und kostenintensiv.

Damit die Ressourcen sinnvoll und effizient eingesetzt werden können, die Zusammenarbeit der Strafverfolgungsbehörden gestärkt wird und ein gezieltes Handeln von Polizei und Staatsanwaltschaft ermöglicht werden kann, ist eine gemeinsame Strategie von Staatsanwaltschaft und Polizei in der Bekämpfung der Cyberkriminalität unabdingbar.

2.2. Ziel der Vorlage

Das Postulat von Postulat: 2017/186: «Kantonale Strategie Cyber-Kriminalität» wird beantwortet und dem Landrat wird eine Strategie dargelegt, die aufzeigt, wie die Polizei Basel-Landschaft und die Staatsanwaltschaft die Delikte aus dem Bereich Cybercrime in Zukunft bekämpfen werden.

Es wird dem Landrat beantragt, die für die Umsetzung der Cybercrime-Strategie erforderlichen finanziellen und personellen Ressourcen bei Polizei und Staatsanwaltschaft zu beschliessen.

Anpassung der Rechtsgrundlagen
Da die Umsetzung der Cybercrime-Strategie der Strafverfolgungsbehörden eine Erhöhung der Zahl der Sollstellen der ordentlichen Staatsanwälte und Staatsanwältinnen um zwei zur Folge hat, ist das Dekret zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (Dekret EG StPO, SGS 250.1) anzupassen.

2.3. Ist-Zustand bei der Bearbeitung von Delikten im Bereich Cybercrime ieS und DigiKrim

2.3.1. Polizei Basel-Landschaft

Delikte im Bereich der Cybercrime ieS und DigiKrim werden in den allermeisten Fällen an den Schaltern der Polizeiposten zur Anzeige gebracht. In wenigen Fällen erfolgt die Meldung direkt bei der Staatsanwaltschaft. Bei der Sicherheitspolizei der Polizei Basel-Landschaft erfolgt eine Bearbeitung der niederschwelligen Fälle von DigiKrim nach bestem Wissen und Gewissen mit rudimentären technischen Kenntnissen. Die Sachbearbeitenden geraten eher zufällig an die Bearbeitung solcher Fälle. Es existieren keine Prozesse oder Abläufe für die Fallbearbeitung. Allenfalls beschafft sich der Sachbearbeiter oder die Sachbearbeiterin Wissen bei Mitarbeitenden der Staatsanwaltschaft, von Ermittlungsdiensten oder der IT-Forensik.

Komplexere Fälle gelangen direkt oder von der Sicherheitspolizei über die Staatsanwaltschaft mittels Auftrag zu den Ermittlungsdiensten der Kriminalpolizei. Ein Mitarbeiter oder eine Mitarbeiterin übernimmt, abhängig von seinen freien Ressourcen und eher zufällig, die Bearbeitung solcher Fälle.

Nur vereinzelte Mitarbeitende der Ermittlungsdienste sowie das Team IT-Forensik verfügen über spezifische Kenntnisse in der Bekämpfung der Cybercrime ieS und DigiKrim. Die Kenntnisse können nicht optimal zur Verfügung gestellt werden, da die Mitarbeitenden verschiedenen Organisationseinheiten unterstehen und eine Koordination zwischen den Mitarbeitenden schwierig ist. Ebenso besteht kein Aus- und Weiterbildungskonzept auf diesem überaus technischen und komplexen Gebiet, das sich laufend weiterentwickelt.

Den ermittelnden Mitarbeitenden von Polizei und Staatsanwaltschaft steht das kleine Team der IT-Forensik, bestehend aus einem Teamleiter, vier Disk-Forensikern und einer Fachfrau für Mobile Devices zur Seite, das versucht, zeitnah mit IT-forensischen Dienstleistungen und Fachwissen bei der Bearbeitung von Cybercrime-Delikten Unterstützung zu leisten. Dieses Team muss auf Grund der Vielzahl von Fällen und Gerätschaften die Aufträge priorisieren. Liegen gehäuft Haftfälle und andere Ereignisse vor, die eine zeitlich bevorzugte Bearbeitung erfordern, können «normaldringliche» Fälle in eine Auswertungsverzögerung von bis zu acht Monaten geraten. Die Wartezeit für die Sicherung von mobilen Geräten (z.B. Smartphones) kann mehrere Wochen dauern. Diese langen Wartezeiten sind von der Staatsanwaltschaft in den vergangenen Jahren wiederholt kritisiert worden, da darunter einerseits die Qualität der Strafverfahren leidet (zumal wenn die weiteren Verfahrenshandlungen [namentlich Einvernahmen etc.] von der IT-Auswertung abhängen und folglich über sehr lange Zeit nicht vorgenommen werden können) und andererseits eine Verletzung des Beschleunigungsgebots (Art. 5 StPO) und als Folge hiervon eine Reduktion des Strafmasses drohen.

2.3.2. Staatsanwaltschaft

Delikte der Cyberkriminalität gehen bei der Staatsanwaltschaft hauptsächlich mittels Anzeige der Polizei ein. Ungefähr 5 bis 10 Prozent der Anzeigen gehen direkt bei der Staatsanwaltschaft ein. Ungefähr gleich viele Anzeigen werden mittels Gerichtsstandsanfragen an die Staatsanwaltschaft Basel-Landschaft abgetreten.

Generell lässt sich sagen, dass in einer Grosszahl der Fälle der DigiKrim, namentlich bei Internetbetrügen (z.B. via Ricardo, Tutti, etc.), Ehrverletzungen und Drohungen übers Internet (z.B. via E-Mail, Facebook, etc.) sowie verbotene Pornographie, die meisten Mitarbeitenden der Staatsanwaltschaft über das erforderliche Fachwissen verfügen, um die bei der Staatsanwaltschaft eingehenden Fälle selbständig oder gegebenenfalls in Zusammenarbeit mit der Polizei (IT Forensik, AED, etc.) untersuchen oder im Pikett «in den ersten Angriff nehmen» zu können. Die Aufklärungsquote ist insoweit ähnlich hoch wie bei den gleichen Delikten, die ohne Zuhilfenahme des Internets begangen werden. Gleichwohl ist bei den Mitarbeitenden auch bereits in diesem Bereich flächendeckend ein (periodischer) Weiterbildungsbedarf auszumachen, um mit den (informations-)technologischen Entwicklungen Schritt zu halten und mit den sich laufend weiterentwickelnden Cybercrime-Phänomenen vertraut zu bleiben.

Bei sämtlichen übrigen Delikten von Cybercrime ieS und von komplexerer DigiKrim verfügen demgegenüber nur wenige Mitarbeitende der Staatsanwaltschaft über das erforderliche Fachwissen, die Fälle zu untersuchen, wobei aber niemand eine (zertifizierte) spezialisierte Ausbildung auf dem Gebiet Cybercrime hat. Die bei der Staatsanwaltschaft eingehenden Fälle von Cybercrime ieS werden in der Regel diesen wenigen Mitarbeitenden zugeteilt. Im Pikett kann das erforderliche Fachwissen nur zum Teil (über die Polizei oder Staatsanwaltschaft-intern) erhältlich gemacht werden. Abgesehen von den erwähnten wenigen Mitarbeitenden fehlt den Pikett-Mitarbeitenden weitgehend das erforderliche Spezialwissen für einen wirksamen ersten Angriff (beispielsweise zum Ergreifen adäquater Zwangsmassnahmen oder zur Einvernahme von «Hackern», etc.).

2.4. Bisher getroffene Massnahmen

Innerhalb des Kantons Basel-Landschaft gibt es sporadisch Weiterbildungen zum Thema Cyberkriminalität. Diese Weiterbildungen werden von Mitarbeitenden besucht, die sich für die Thematik interessieren und eignen. Letzteres gilt auch für ausserkantonale Weiterbildungen.

Die Polizei Basel-Landschaft hat mit Reorganisation und Strukturänderungen die Präsenz der Polizei in der Bevölkerung erhöht, um damit die gesteckten Ziele, z.B. in der Thematik Einbruchsprävention und der Steigerung der Aufklärungsraten bei Einbruchdiebstählen und schweren Gewaltdelikten, zu erreichen. Erfolge konnten nur mit grossem personellem Aufwand über alle Bereiche der Polizei erreicht werden. Dabei zeigte sich, dass in weiteren Bereichen wie Lage- und Informationszentrum, Forensik, Observation, Nachrichtendienst und Social Media Personal fehlt. So sind nicht nur die operativen Elemente bis zum Anschlag gefordert, sondern auch rückwärtige Bereiche. Im Support (IT etc.) sind Ressourcenengpässe zu verzeichnen, die negative Auswirkungen auf das operative Geschäft nach sich ziehen.

2.5. Voraussetzungen für eine erfolgreiche Bekämpfung von Cyberkriminalität

Die Bekämpfung bzw. die Bearbeitung von DigiKrim und Cybercrime ieS durch die Polizei Basel-Landschaft benötigt interdisziplinäres Wissen, basierend auf Ausbildungen der höheren Fachschulen, Fachhochschulen und Universitäten. Die technische Komplexität ist sehr hoch und benötigt Fachspezialisten und Fachspezialistinnen, die nicht aus den Reihen der Polizei rekrutiert werden können. Dies trifft insbesondere in den Themenfeldern IT-Forensik und IT-Überwachung zu. Nur im Bereich der IT-Ermittlung ist eine Schulung und Spezialisierung von bestehenden Ermittlungsressourcen denkbar. Somit ist es unabdingbar, neue Stellen mit qualifizierten Spezialisten zu schaffen. Somit ist es zwingend Spezialisten für die Bewältigung dieser Aufgaben, wie auch für die interne Aus- und Weiterbildung zu rekrutieren.

Auch seitens der Staatsanwaltschaft ist eine fundierte Ausbildung, bzw. ein fundiertes Wissen, auf dem Gebiet der digitalisierten Kriminalität und von Cybercrime erforderlich. Die Verfahrensleitung solcher Fälle braucht ein hohes technisches Verständnis, juristische Kenntnisse, Erfahrung und eine gehörige Portion Zeit. Verfahren aus dem Bereich DigiKrim und Cybercrime ieS lösen durch die Art der Delikte und den eingesetzten Technologien umfangreiche Abklärungen und teilweise kantonale und internationale Rechtshilfeersuchen aus. Diese «step-by-step» Ermittlungen sind bei der Polizei und Staatsanwaltschaft stets mit einem sehr grossen Aufwand verbunden. Gleichzeitig ist festzuhalten, dass ohne diesen Aufwand eine Steigerung der Aufklärungsrate bei Fällen von DigiKrim und Cybercrime ieS nicht möglich ist.

2.6. Gemeinsame Strategie Polizei Basel-Landschaft/Staatsanwaltschaft

Aufgrund der strategischen Vorgaben (vgl. Ziff. 2.4) innerhalb des Kantons Basel-Landschaft sowie aufgrund der bisherigen Erkenntnisse aus dem Projekt Cybercrime, der Auswertung der Bevölkerungsumfrage und den Schlussfolgerungen aus dem Bericht der Finanzkontrolle (vgl. Ziff. 2.1.12) ergibt sich, dass Polizei und Staatsanwaltschaft gehalten sind, eine Organisationsstruktur aufzubauen, die auf aktuelle und künftige Herausforderungen im Cybercrime-Bereich effektiv und effizient reagieren kann. Im Rahmen der Umsetzung einer den vorerwähnten Anforderungen entsprechenden Strategie steht als erstes eine gezielte fachliche Spezialisierung bei Polizei und Staatsanwaltschaft mit einem entsprechenden signifikanten Know-How-Aufbau. Dazu werden bei Polizei und Staatsanwaltschaft Mitarbeitende zu Cybercrime-Fachspezialisten weitergebildet, die innerhalb eines Fachteams Fälle von Cyberkriminalität bearbeiten.

Eine gemeinsame Strategie beinhaltet, dass in den vier Bereichen «Aus- und Weiterbildung», «Spezialisierung», «Repression» und «Prävention» Massnahmen getroffen werden müssen, um die Cyberkriminalität wirksam(er) bekämpfen zu können. Dementsprechend wurden vier strategische Stossrichtungen formuliert, die wie folgt als **Vier-Pfeiler-Modell** dargestellt werden können:

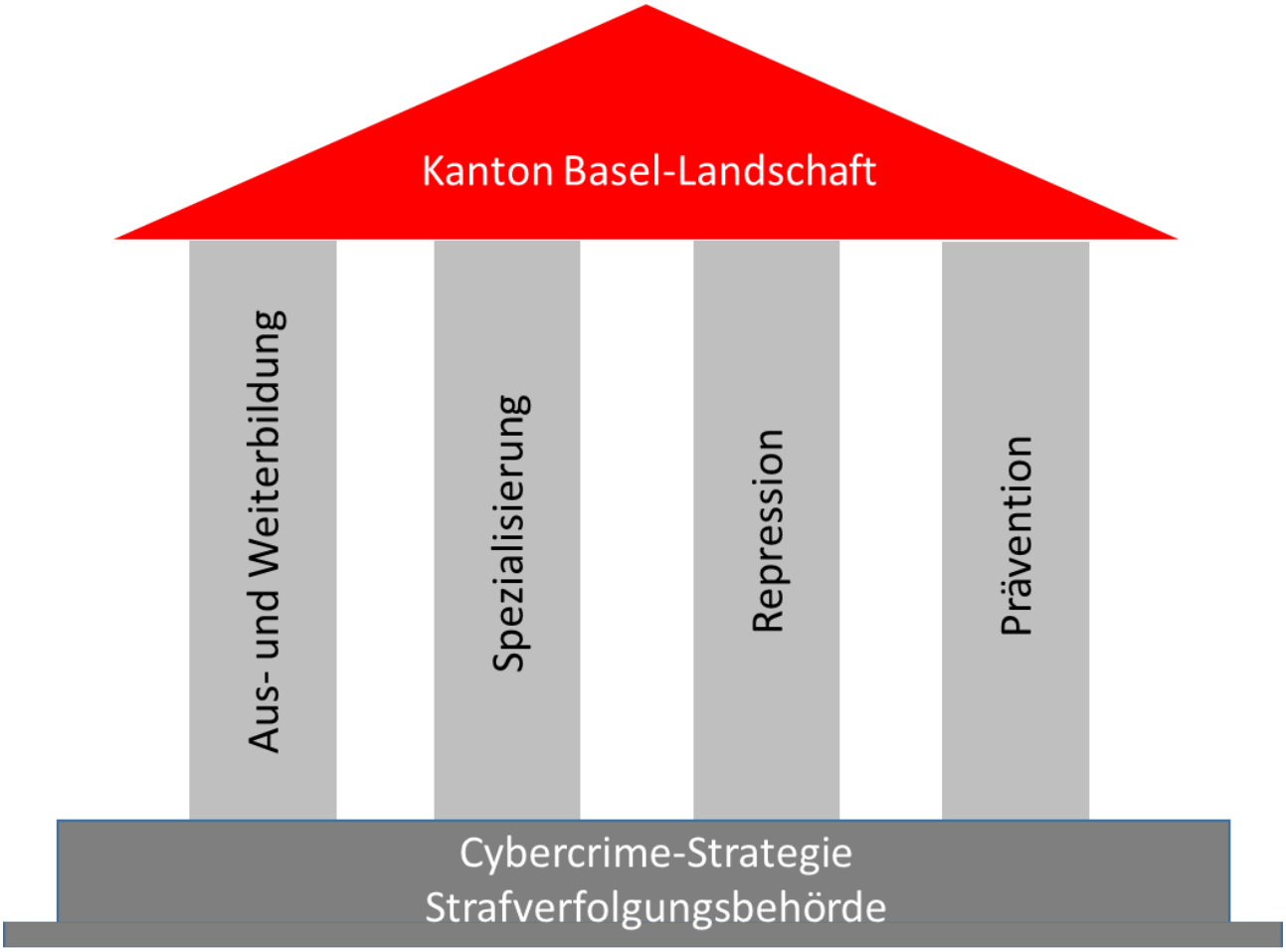

Abb. 2: Vier-Pfeiler-Modell der Cybercrime-Strategie BL

I. AUS- UND WEITERBILDUNG

Polizei und Staatsanwaltschaft werden auf allen Stufen im Bereich Cyberkriminalität geschult. Da DigiKrim in praktisch allen Bereichen des Strafrechts vorkommt, müssen grundsätzlich alle Mitarbeitenden (zumindest) in der Anfangsphase der Untersuchung in der Lage sein, Fälle von DigiKrim zu bearbeiten. Die spezialisierten Teams der Polizei und Staatsanwaltschaft (vgl. Pfeiler II) sind für die Schulung sämtlicher Mitarbeitenden dieser beiden Dienststellen sowie der Jugendanwaltschaft besorgt und zeichnen dafür verantwortlich, dass sie über das erforderliche Grundwissen verfügen, hinreichend Fachspezialisten und Fachspezialistinnen zur Verfügung stehen, periodische Aus- und Weiterbildungen durchgeführt werden und Networking sowie Austausch mit Lehre und Forschung etc. betrieben werden. Dabei wird auch dem Know-how-Transfer innerhalb der Organisationen Polizei und Staatsanwaltschaft sowie organisationsübergreifend eine grosse Bedeutung beigemessen.

II. SPEZIALISIERUNG

Bei Polizei und Staatsanwaltschaft existieren spezialisierte Teams, die Fälle von Cybercrime ieS sowie umfangreichere und komplexere Fälle von DigiKrim untersuchen und erledigen. Die Mitarbeitenden dieser Teams sind in der Cybercrime-Ermittlung qualifiziert ausgebildet oder verfügen über eine gleichwertige Berufserfahrung. Die Teams sind nebst der Fallbearbeitung (vgl. Pfeiler III) für die Aus- und Weiterbildung der übrigen Mitarbeitenden von Polizei und Staatsanwaltschaft und Jugendanwaltschaft (vgl. Pfeiler I) sowie für die Prävention (vgl. Pfeiler IV) besorgt. Ebenfalls leisten sie fachlichen Support in Fällen von DigiKrim, die von den übrigen Mitarbeitenden der Polizei und Staatsanwaltschaft bearbeitet werden.

III. REPRESSION

Die spezialisierten Teams von Polizei und Staatsanwaltschaft (vgl. Pfeiler II) sind im Rahmen der ihnen gewährten Möglichkeiten und Mittel dafür besorgt, in den ihnen zugeteilten Cybercrime-Fällen die Täterschaft zu ermitteln und für eine gleichmässige Durchsetzung des staatlichen Strafanspruchs zu sorgen. In den Deliktsfeldern Cybercrime ieS und umfangreicherer und komplexerer DigiKrim sind sie, gegebenenfalls in Zusammenarbeit mit weiteren Partnerstellen, darum bemüht, die Aufklärungsquote sowie die Anzahl Erledigungen zu erhöhen bzw. im interkantonalen Vergleich auf überdurchschnittlich hohem Niveau zu halten. Die Bewältigung komplexerer Verfahren im Cybercrime-Bereich wird sichergestellt. Die Prozesse innerhalb von Polizei und Staatsanwaltschaft werden zur Steigerung der Verfahrenseffizienz vereinheitlicht und koordiniert. Verstärkte Zusammenarbeit mit anderen Kantonen, dem Bund und dem Ausland (internationale Kooperation bei transnationalen Fallkomplexen) wird angestrebt.

IV. PRÄVENTION

Fälle von Cyberkriminalität werden bereits bei Eingang der Anzeige als solche gekennzeichnet und erfasst. Die spezialisierten Teams von Polizei und Staatsanwaltschaft (vgl. Pfeiler II) werden über sämtliche Fälle von Cyberkriminalität (zumindest) in Kenntnis gesetzt. Die spezialisierten Teams analysieren und dokumentieren laufend die Phänomene der Cyberkriminalität (Bewirtschaftung Phänomene- und Leistungskatalog). Sie informieren die Bevölkerung regelmässig sowie bei Bedarf über aktuelle und neue Cybercrime-Phänomene und geben ihr konkrete Tipps, um nicht Opfer von Cyberkriminalität zu werden. Die Polizei stärkt mit Blick auf globale Bedrohungen das subjektive Sicherheitsgefühl der Bevölkerung mittels einer verstärkten Zusammenarbeit mit Privaten. Das Angebot an Online-Dienstleistungen, namentlich im Bereich Social Media wird ausgebaut, damit die Bevölkerung zeitnah informiert werden kann. Eine aktive Prävention, beispielsweise die Durchführung von Infoveranstaltungen an Schulen, wird betrieben. Die Stärkung des Informationsaustausches mit Privaten, insbesondere mit Cyber-Dienstleistern, wird angestrebt.

2.7. Organisationsformen bei Polizei und Staatsanwaltschaft für die Umsetzung der Strategie

Im Projekt Cybercrime wurden eine Analyse und Bewertung durchgeführt, um die für die formulierten Ziele angemessene Organisation der spezialisierten Teams zu eruieren. Dabei setzte sich das Projektteam intensiv mit mehreren Organisationsformen auf Ebene Polizei und Staatsanwaltschaft auseinander und berücksichtigte auch Erfahrungen von bereits bestehenden Cybercrime-Einheiten der Strafverfolgung.

2.7.1. Polizei

Analyse und Bewertung ergaben, dass die Mitarbeitenden in einer eigenständigen Organisationseinheit zusammenzufassen sind. Aus Sicht der Polizei ist entscheidend, dass sich eine Organisationseinheit im Kompetenzbereich Cybercrime (mit den Bereichen IT-Forensik, IT-Ermittlung und IT-Überwachung) spezialisieren kann. Die Bearbeitung von Cybercrime deckt alle Bereiche ab. Mitarbeitende der IT-Forensik sollen Ermittlungsarbeiten und IT-Ermittler sollen Tätigkeiten im Bereich der IT-Forensik ausführen können. Der Bereich der IT-Überwachung hat an Bedeutung stark zugenommen. Die Herausforderungen für eine moderne und zielführende Überwachung liegen heute im Bereich des Internets bzw. den Geräten, die durch die Täterschaft benutzt werden, um über das Internet zu kommunizieren. Die Sachverhalte sind teilweise äusserst komplex und aufgrund der möglichen technischen Komponenten zeigen sich immer wieder neue Konstellationen, die zu bewältigen sind. Die Erfahrungen von Strafverfolgungsbehörden, die sich im Bereich Cybercrime bereits neu organisiert haben, sprechen ebenfalls klar für eine Zusammenfassung der verschiedenen Bereiche in eine Organisationseinheit. Für eine eigenständige Organisationseinheit spricht im Weiteren, dass diese einen 24/7-Pikettdienst sowie eine Hotline (während der Bürozeiten) aufrechterhalten kann. Die Kontaktpflege und das wichtige Networking können ebenfalls durch diese Organisationseinheit sichergestellt werden. Die Organisationseinheit soll als eigene Abteilung aufgebaut werden.

2.7.2. Staatsanwaltschaft

Analyse und Bewertung ergaben, dass innerhalb der Staatsanwaltschaft die Gründung eines Fachbereichs, dessen Mitarbeitende einerseits Fälle von Cybercrime ieS sowie komplexere und umfangreichere Fälle von DigiKrim selber untersuchen und zum strafprozessualen Abschluss bringen und andererseits je nach Kapazität auch andere Fälle untersuchen, am flexibelsten und am besten geeignet erscheint. Die Vorteile dieser Organisationsform liegen darin, dass mit einem zu Beginn der Umsetzung der Strategie relativ kleinen, aber spezialisierten Team innerhalb der bestehenden Strukturen der Staatsanwaltschaft gearbeitet werden kann, mit welchem flexibel die anfallenden Aufgaben erledigt werden können und welches bei Bedarf auch ausgebaut werden kann. Der Fachbereich wird der Hauptabteilung Betäubungsmittelkriminalität und organisierte Kriminalität (HA BM/OK) angegliedert, da die Untersuchungsmethoden im Bereich Cybercrime i.e.S. sehr ähnlich sind wie in den Deliktsbereichen, in denen die HA BM/OK bereits tätig ist.

Bei der Bekämpfung der Cyberkriminalität ist oftmals schnelles Handeln entscheidend für den Erfolg, zumal regelmässig Sofortmassnahmen (z.B. Hausdurchsuchungen, Sicherung von Daten mittels Rechtshilfeersuchen gestützt auf die Cybercrime-Convention, etc.) einzuleiten sind. Hierzu ist ein rascher persönlicher Austausch zwischen Polizei und Staatsanwaltschaft erforderlich. Idealerweise sollten die beiden Einheiten unter einem Dach ansässig sein. Das Kompetenzzentrum Cybercrime der Staatsanwaltschaft Zürich hat die räumliche Nähe zur Polizei wiederholt als wichtigen Erfolgsfaktor bezeichnet.

2.8. Konkrete Auswirkungen auf die Organisationen der Polizei und der Staatsanwaltschaft/Ressourcen

2.8.1. Polizei Basel-Landschaft: Abteilung Cybercrime

Der Ausbau hin zum Soll-Bestand und zur Abteilung Cybercrime wird nach einem zustimmenden und rechtskräftig gewordenen Entscheid des Landrats vorgenommen.

Organigramm

Die neue Abteilung Cybercrime fügt sich wie folgt in die Organisation der Polizei Basel-Landschaft ein:

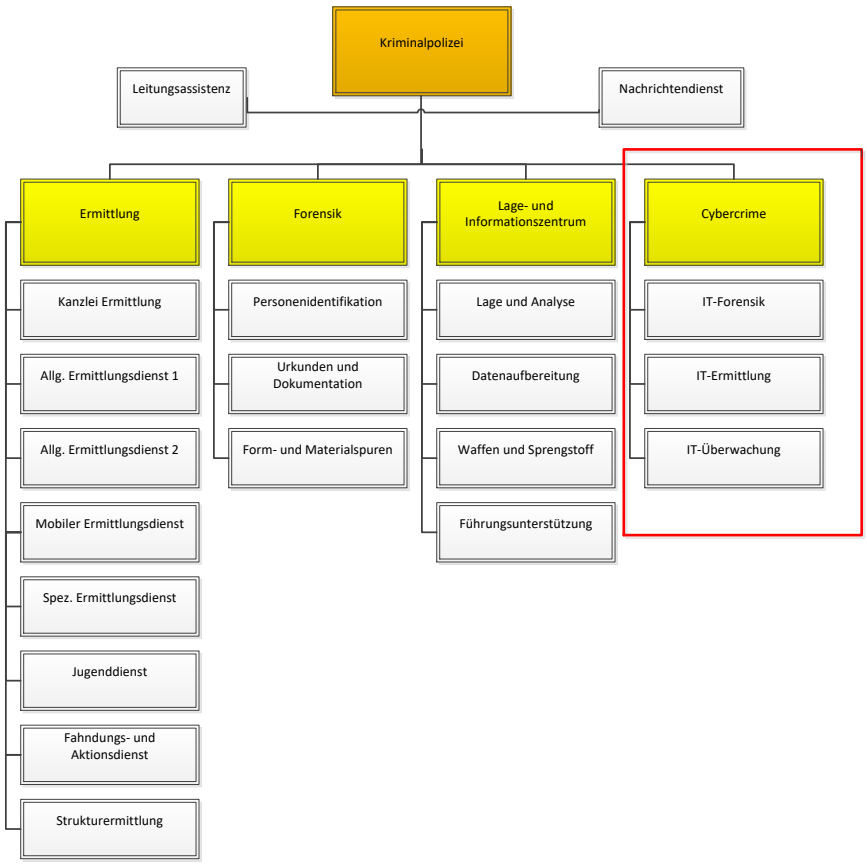

Abb. 3: Künftiges Organigramm der Polizei mit der Abteilung Cybercrime

Personelle Ressourcen

Zur Bekämpfung von DigiKrim und Cybercrime ieS werden schon jetzt und angesichts des kontinuierlichen Anstiegs der Cyberkriminalitätsfallzahlen auch in Zukunft zunehmend Ressourcen der gesamten Polizei benötigt. Diese Delikte werden auch zur Anzeige gebracht, verbunden mit den Erwartungen der geschädigten Bevölkerung, dass ihre Ereignisse professionell angegangen werden. Angefangen bei der Anzeigenerstattung, der Rapportierung und den anschliessenden Vorermittlungen, über die Weitergabe der Fälle an Ermittlungsdienste, Staatsanwaltschaft und Spezialisten und Spezialistinnen der künftigen Abteilung Cybercrime bei der Polizei, bzw. dem Fachbereich Cybercrime bei der Staatsanwaltschaft, beschäftigt sich jeder Bereich mit diesen Delikten. Jeder vorgängig genannte Bereich muss konstant für diese Aufgabe geschult werden, so dass eine fachlich und rechtlich korrekte Bearbeitung dieser Fälle erfolgen kann. Damit wird eine Erhöhung der Aufklärungsrate wahrscheinlich. Durch die Schaffung der Abteilung Cybercrime werden in den angestammten Bereichen der Polizei (Sicherheitspolizei und Kriminalpolizei) keine Ressourcen frei. Diese werden wie bisher mit der Bearbeitung der Fälle beschäftigt sein, jedoch unterstützt durch die Spezialisten der Abteilung Cybercrime. Nur so ist erreichbar, dass die Abteilung Cybercrime sowohl die Polizei als auch den Fachbereich Cybercrime der Staatsanwaltschaft mit Dienstleistungen unterstützen als auch komplexe Ermittlungsverfahren selber durchführen kann.

Im Bereich der IT-Forensik nehmen die Fragestellungen, die sich bei der Sicherung, Aufbereitung, Auswertung und Dokumentationen der gesicherten Datenbestände ergeben, je länger je mehr an Komplexität zu. Daraus resultiert ein erheblicher personeller Mehraufwand. In den Bereichen Fahrzeug-Forensik sowie Internet of Things-Forensik kommen komplexe neue Aufgabenfelder hinzu und die Möglichkeiten der Cloud nehmen im Geschäfts- und Privatbereich einen immer grösseren Stellenwert ein.

Im Rahmen von verdeckten Überwachungen wird IT-Wissen unabdingbar. Aufgrund des rasanten technischen Fortschrittes müssen Applikationen und Tools, die der Überwachung dienen, stetig weiterentwickelt und eingeführt werden. Die Anwender müssen geschult und unterstützt werden, was wiederum einen erheblichen personellen Aufwand bedeutet.

Auf Grund dieser Gesamtsituation kann die Besetzung der neuen Abteilung Cybercrime mit den erforderlichen Stellenprozenten nicht intern erfolgen, weshalb zusätzliche Personalressourcen für die Bekämpfung von Cybercrime notwendig sind (vgl. auch die Ausführungen unter 2.1.13.).

Der Soll-Bestand (personelle Ressourcen) basiert auf den Berechnungen der Personentage aus der Aufgaben- und Stunden-Berechnung sowie den Erfahrungswerten der IT-Forensik und der Mitarbeitenden, die sich bereits teilweise mit IT-Ermittlung und IT-Überwachung beschäftigt haben.

Der ermittelte Bedarf an personellen Ressourcen bis zum vollständigen Ausbau der Abteilung Cybercrime setzt sich wie folgt zusammen:

Fachgebiet/Tätigkeit	**PT**	**MA**
Personentage Leitung	212	1.00
Personentage Hotline	249	1.17
Personentage IT-Forensik	2529	11.93
Personentage IT-Ermittlung	1020	4.81
Personentage IT-Überwachung	252	1.19
Personentage Ausbildertätigkeit	50	0.24
Total	4312	20.34
Mehrbedarf Mitarbeitende		**13.34**

Die Abteilung Cybercrime soll im Endausbau einen Personalbestand von 20 Vollzeitstellen aufweisen. Das bedeutet, dass zusätzlich 13 neue Stellen zu schaffen sind.

Die Stellen werden innerhalb von vier Jahren (abzustimmendem Landratsbeschluss) wie folgt eingeführt:

Stellen/Profile	Bestand	Zusatzbedarf				Summe
	2019	2020	2021	2022	2023	
AL Cybercrime	-	100%	-	-	-	100%
IT-Forensik	700%	100%	100%	200%	100%	1200%
IT-Ermittlung	-	200%	100%	100%	100 %	500%
IT-Überwachung	-	-	100%	100%	-	200%
Summe	**700%**	**400%**	**300%**	**400%**	**200%**	**2000%**

Die Abteilung Cybercrime wird von einem Abteilungsleiter oder einer Abteilungsleiterin geführt. Im Weiteren wird ein Dienstleiter oder eine Dienstleiterin den Dienst IT-Forensik leiten. Die IT-Forensik wird aus insgesamt 11 Mitarbeitenden bestehen. Ein Teamleiter oder eine Teamleiterin IT-Ermittlung wird ein Team von vier IT-Ermittlern und IT-Ermittlerinnen führen. Das Team der IT-Überwachung wird aus zwei Personen bestehen.

Die folgenden Kompetenzen sind nach der Umsetzung vorhanden:

Kompetenzniveau	Aufgabenbeschreibung
Sachbearbeitung Niveau I	Die Sachbearbeitenden sind grundsätzlich in der Lage, bei Cyberdelikten (Cybercrime ieS und DigiKrim) den Sachverhalt richtig zu erfassen, aufzunehmen und anschliessend korrekt zu rapportieren. Sie informieren bei den definierten Cyberdelikten (i.d.R. Cybercrime ieS) die Abteilung Cybercrime und stellen damit die korrekte Weiterbearbeitung des Falles sicher. Als Hilfsmittel stehen Phänomeneblätter zur Verfügung. Die fachliche Unterstützung der Sachbearbeitenden Niveau I wird einerseits durch die Multiplikatoren, anderseits durch die Hotline der Abteilung Cybercrime gewährleistet.
Sachbearbeitung Niveau II	Die Sachbearbeitenden Niveau II verfügen nach erfolgter Ausbildung im Bereich Cybercrime Niveau II (SPI, interne Ausbildung) über ein breites Fachwissen. Dadurch sind sie grundsätzlich in der Lage, Cyberdelikte zu erkennen und korrekt zu bearbeiten. Bei kriminalpolizeilichen Ermittlungen bzw. Aufträgen der Staatsanwaltschaft handelt es sich in der Regel um Fälle von DigiKrim. Die fachliche Unterstützung erhalten die Sachbearbeitenden Niveau II direkt von der Abteilung Cybercrime.
Sachbearbeitung Niveau III	Die Sachbearbeitenden Niveau III verfügen über ein Fachwissen auf Niveau III oder höher, sei dies durch gezielte Fort- und Weiterbildung als auch durch entsprechende Berufserfahrung und/oder höhere Berufsabschlüsse.

Kompetenzniveau	Aufgabenbeschreibung
Sachbearbeitung Niveau III, IT-Forensik	Die Sachbearbeitenden Niveau III, IT-Forensik, haben folgende Kernaufgaben: • Forensische Sicherung und Aufbereitung von klassischen Rechnersystemen und Mobile Devices • Forensische Sicherung von Webseiten, Foren etc. • Logfile, Header- und Malwareanalyse • Fachliche Unterstützung der Sachbearbeitenden der Niveaus I-III in Fragen betreffend IT-Forensik • Betreiben der Hotline Cybercrime • Ausbildertätigkeit Intern/Extern • Betreiben von eigener Fortbildung und Networking • Fahrzeugforensik • Weitere forensische Datensicherung (z.B. Internet of Things)
Sachbearbeitung Niveau III, IT-Ermittlung	Die Sachbearbeitenden Niveau III, IT-Ermittlung, haben folgende Kernaufgaben: • Betreiben eigener Ermittlungen im Bereich von Cybercrime ieS und in komplexen Fällen von DigiKrim • Fachliche Unterstützung der Sachbearbeitenden Niveau I & II im Bereich von IT-Ermittlungen • Betreiben der Hotline Cybercrime • Patrolling/Monitoring • Ausbildertätigkeit Intern/Extern • Präventionstätigkeit • Betreiben von eigener Fortbildung und Networking
Sachbearbeitung Niveau III, IT-Überwachung	Die Sachbearbeitenden Niveau III, IT-Überwachung, haben folgende Kernaufgaben: • Technische Betreuung/Administrierung von Überwachungssystemen • Betreiben von sonstigen technischen Massnahmen • Betreuung und Support der Bundesapplikationen der Ermittlung. Unterstützung bei der Weiterentwicklung von Bundesapplikationen • Einsatz von Kommunikationsüberwachungssystemen (Art. 269 ff. StPO und Art. 280 StPO) • Fachliche Unterstützung der Sachbearbeitenden Kripo im Bereich von IT-Überwachung • Betreiben der Hotline Cybercrime • Ausbildertätigkeit intern/extern • Betreiben von eigener Fortbildung und Networking

Die Zuständigkeiten und Aufgaben der Abteilung Cybercrime sind in der nachfolgenden Tabelle aufgeführt:

#	Aufgaben	Beschreibung	Strategiebezug
1	Cybercrime ieS	Die Mitarbeitenden der Abteilung Cybercrime sind innerhalb der Polizei Basel-Landschaft grundsätzlich für die Bearbeitung von Cybercrime ieS zuständig. Die Ermittlungen werden nach Massgabe der Staatsanwaltschaft geführt. Der Leiter der Abteilung Cybercrime entscheidet abschliessend über die Zuständigkeit und Bearbeitung der Fälle von Cybercrime ieS.	Spezialisierung Repression
2	Umfangreichere und komplexere Fälle von DigiKrim	Die Mitarbeitenden der Abteilung Cybercrime sind innerhalb der Polizei Basel-Landschaft grundsätzlich für die Bearbeitung von umfangreicheren und komplexeren Fällen von DigiKrim zuständig. Die Ermittlungen werden nach Massgabe der Staatsanwaltschaft geführt. Der Leiter der Abteilung Cybercrime entscheidet abschliessend über die Zuständigkeit und Bearbeitung der Fälle von DigiKrim.	Spezialisierung Repression
3	Betrieb eines fachlichen Pikettdienstes via Hotline	Betrieb der Hotline Cybercrime durch die Mitarbeitenden der Abteilung Cybercrime. Diese Hotline soll für die Mitarbeiter im Korps und für externe Partner erste Ansprechstation im Bereich von Cybercrime ieS und DigiKrim sein.	Spezialisierung Repression
4	IT-Forensik Datensicherung	Die Mitarbeitenden der IT-Forensik sind für die forensische Datensicherung bei klassischen Rechnersystemen, Mobile Devices, IoT, Cloud und Fahrzeugen etc. zuständig.	Spezialisierung Repression
5	IT-Forensik Aufbereitungsmassnahmen	Die Mitarbeitenden der IT-Forensik sind für die Aufbereitungsmassnahmen der forensisch gesicherten Abbilder aus Rechnersystemen, Mobile Devices, IoT, Cloud und Fahrzeugen etc. zuständig.	Spezialisierung Repression
6	IT-Forensik Weitere Tätigkeiten	Die Mitarbeitenden der IT-Forensik sind für die Sicherung von Webseiten und Foren, Multimedia-Forensik, Logfile-, Header- und Malware-Analyse zuständig. Bei Bedarf können Mitarbeitende der IT-Ermittlung zugezogen werden.	Spezialisierung Repression
7	IT-Überwachung Technische Betreuung, Administration Überwachungssysteme des Bundes	Die Mitarbeitenden der IT-Überwachung sind für die technische und administrative Betreuung der (Bundes-) Überwachungssysteme, deren Administration sowie für die Betreuung der mit Überwachungsmassnahmen betrauten Mitarbeitenden der Kripo zuständig.	Spezialisierung Repression
8	IT-Überwachung Kommunikationsüberwachungssysteme	Die Mitarbeitenden der IT-Überwachung sind für die technischen, organisatorischen sowie administrativen Belange rund um den Einsatz von Kommunikationsüberwachungssystemen (Art. 269 ff. und 280 StPO) zuständig.	Spezialisierung Repression
9	Aus- und Weiterbildung Cybercrime innerhalb und ausserhalb der Polizei	Die Mitarbeitenden der Abteilung Cybercrime beteiligen sich als Referenten/Dozenten für Aus- und Weiterbildungen im Bereich Cybercrime innerhalb der Polizei Basel-Landschaft und bei Partnerorganisationen. Nach Möglichkeit werden Aus- und Weiterbildungen in Zusammenarbeit mit dem Fachbereich Cybercrime der Stawa	Aus- und Weiterbildung

#	Aufgaben	Beschreibung	Strategiebezug
		durchgeführt.	
10	Eigene Fortbildung	Die Mitarbeitenden der Abteilung Cybercrime bilden sich in ihrem Fachgebiet fort, um den künftigen Anforderungen Rechnung tragen zu können.	Spezialisierung
11	Präventionsarbeit im Bereich Cybercrime	Die Mitarbeitenden der Abteilung Cybercrime unterstützen/beraten die Mitarbeitenden der Prävention, des Jugenddienstes sowie weiterer interner und externer Partner nach Möglichkeit bei deren Präventionsmassnahmen.	Prävention
12	Networking	Die Mitarbeitenden der Abteilung Cybercrime betreiben aktiv Networking zu innerkantonalen, nationalen und internationalen Fachstellen, Gremien und Organisationen.	Spezialisierung
13	Schnittstelle zum Fachbereich Cybercrime der Staatsanwaltschaft	Die Zusammenarbeit mit der Staatsanwaltschaft ist grundsätzlich in der Strafprozessordnung geregelt. Wie in der Cybercrime-Strategie BL ausgeführt, sind die spezialisierten Teams von Pol und Stawa im Rahmen der ihnen gewährten Möglichkeiten und Mittel dafür besorgt, in den ihnen zugeteilten Cybercrime-Fällen die Täterschaft zu ermitteln und für eine gleichmässige Durchsetzung des staatlichen Strafanspruchs zu sorgen. Konkrete Abläufe und Prozesse betreffend die Zusammenarbeit zwischen der Staatsanwaltschaft und der Polizei werden in der Phase Realisierung erarbeitet.	Spezialisierung

Die Aufgaben der Polizei auf dem wichtigen Gebiet der Prävention sind in einem Präventionskonzept enthalten.

Die Aus- und Weiterbildung im Bereich Cybercrime ist im Ausbildungskonzept ausführlich dargelegt.

<u>Weitere Ressourcen</u>
Nebst den personellen Ressourcen werden für die zusätzlichen Stellen weitere Räumlichkeiten erforderlich sein (vgl. dazu Ziff. 2.9). Hinzukommen werden weitere Beschaffungs und wiederkehrende Kosten (Arbeitsplätze, Informatik, Fahrzeuge).

2.8.2. Staatsanwaltschaft: Fachbereich Cybercrime

2.8.2.1. Einleitung

Abgeleitet aus den vier Pfeilern der bereits erläuterten Cybercrime-Strategie erscheint auf Seiten der Staatsanwaltschaft, wie erwähnt, die Gründung eines auf Cybercrime-Delikte spezialisierten Fachbereichs am besten geeignet, den derzeitigen und künftigen Herausforderungen und Formen der Cyberkriminalität kurz- und mittelfristig wirksam entgegen zu treten.

2.8.2.2. Organisation des Fachbereichs Cybercrime

Die Staatsanwaltschaft Basel-Landschaft wird von der Ersten Staatsanwältin geleitet und umfasst insgesamt sechs Hauptabteilungen. Gemäss Entscheid der Geschäftsleitung der Staatsanwaltschaft vom 28. November 2018 ist geplant, den zu gründenden Fachbereich Cybercrime organisatorisch und personell der Hauptabteilung Betäubungsmittelkriminalität und organisierte Kriminalität (HA BM/OK) anzugliedern. Dies auf Grund der Tatsache, dass Art und Inhalt der Ermittlungen sowie auch die einzusetzenden Ermittlungsmethoden gerade bei Cybercrime ieS mit den Ermittlun-

gen der HA BM/OK vergleichbar sind. Personell soll der Fachbereich Cybercrime aus zwei Staatsanwälten und Staatsanwältinnen und vier Untersuchungsbeauftragten bestehen, wobei die Hälfte dieses Stellenbedarfs durch interne Verschiebungen abgedeckt wird. Parallel zum geplanten gestaffelten Ausbau der Abteilung Cybercrime der Polizei ist je nach Fallzahlenentwicklung vorgesehen, den Fachbereich Cybercrime später allenfalls weiter auszubauen.

Der Fachbereich Cybercrime soll als weitgehend eigenständiges Team in die HA BM/OK eingebettet werden. Er soll von einem Staatsanwalt oder einer Staatsanwältin geleitet werden, welchem bzw. welcher die weiteren Fachbereichs-Staatsanwälte, -Staatsanwältinnen und -Untersuchungsbeauftragten personell unterstellt sind, wobei der fachbereichsleitende Staatsanwalt bzw. die fachbereichsleitende Staatsanwältin selber in fachlicher und personeller Hinsicht dem zuständigen Leitenden Staatsanwalt unterstellt ist.

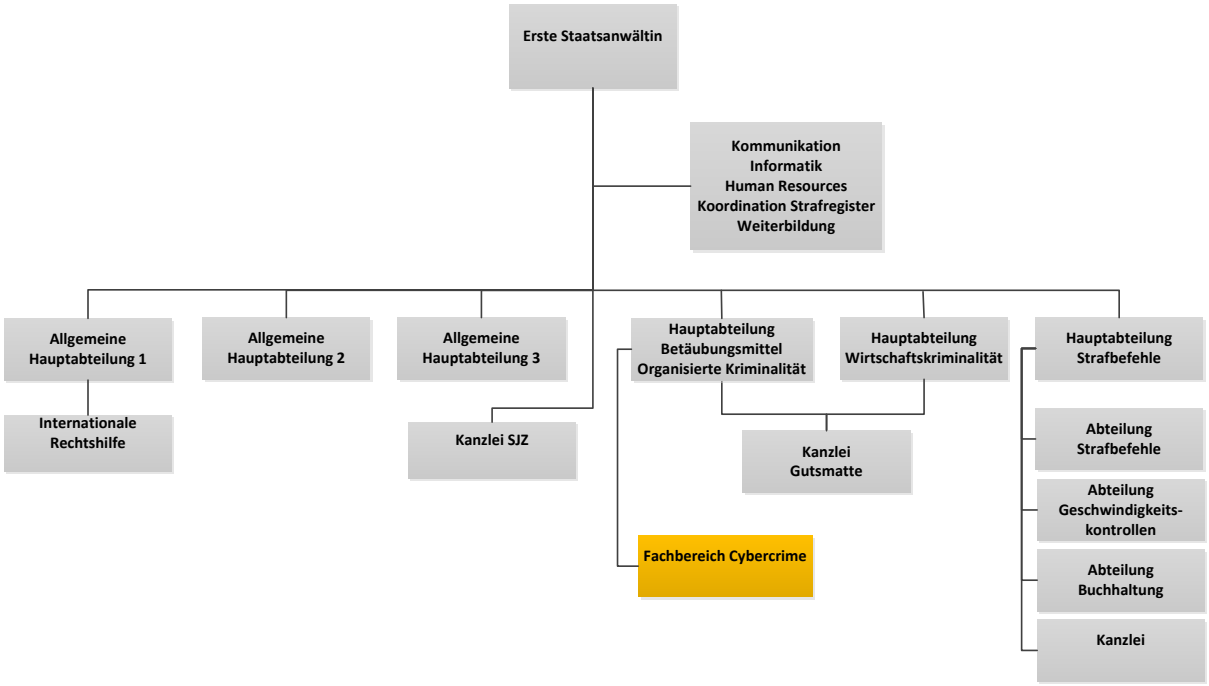

Abb. 4: Künftiges Organigramm der Staatsanwaltschaft mit dem Fachbereich Cybercrime

2.8.2.3. Aufgaben und Zuständigkeiten des Fachbereichs Cybercrime
a. Allgemeines

Gestützt auf die erwähnten vier strategischen Stossrichtungen im Bereich Cyberkriminalität werden sich für den Fachbereich Cybercrime inhaltlich vor allem zwei thematische Schwerpunkte ergeben:

Die Bearbeitung der ihm zugewiesenen Cybercrime-Fälle sowie die Aus- und Weiterbildung. Dabei wird sich Letztere nicht allein auf den Fachbereich selber beschränken, sondern der Fachbereich wird im Bereich Cybercrime ieS und DigiKrim für die Aus- und Weiterbildung der gesamten Staatsanwaltschaft sowie der Jugendanwaltschaft zuständig sein.

Als Folge der Cybercrime-Strategie des Kantons Basel-Landschaft ist auf allen Ebenen der Staatsanwaltschaft stufengerecht eine Spezialisierung zur adäquaten Verfolgung der Cyberkriminalität zu erreichen. Vorgesehen ist, dass der Fachbereich Cybercrime, wie schon erwähnt, denn auch «nur» Fälle von Cyberkriminalität ieS sowie umfangreichere und komplexere Fälle von DigiKrim bearbeitet. Zumal die Cyberkriminalität mittlerweile beinahe sämtliche Deliktsbereiche durchdringt, sollen sämtliche übrigen Fälle mit digitalem Bezug, deren Bearbeitung kein spezialisiertes IT-Wissen erfordert, auch weiterhin durch die übrigen Abteilungen der Staatsanwaltschaft

untersucht werden. Es ist jedoch durch den Fachbereich Cybercrime zu gewährleisten, dass dementsprechend sämtliche Mitarbeitende der Staatsanwaltschaft über die hierfür erforderliche Ausbildung verfügen und namentlich laufend über neue Cybercrime-Phänomene informiert werden.

Um die Qualität der Strafverfolgung in sämtlichen Bereichen der Cybercrime ieS und DigiKrim auf allen Stufen zu verbessern, wird der Fachbereich zudem eine Hotline betreiben, die einerseits innerhalb der Staatsanwaltschaft sowie für die Jugendanwaltschaft als Anlaufstelle für Fragen aus dem Bereich Cybercrime fungiert; andererseits wird sie die Schnittstelle für Anfragen der Abteilung Cybercrime der Polizei bilden. Der Betrieb der Hotline dürfte grundsätzlich einen hohen und namentlich in der Anfangsphase nach der Betriebsaufnahme, wie die entsprechenden Erfahrungen des Kompetenzzentrums der Staatsanwaltschaft des Kantons Zürich mit ihrer in Betrieb genommenen Hotline zeigen, einen sehr hohen Arbeitsaufwand generieren.

b. Fallbearbeitung

Der Fachbereich Cybercrime wird für die Untersuchung und den Abschluss von Fällen aus dem Bereich Cybercrime ieS sowie von umfangreicheren und komplexeren Fällen von DigiKrim zuständig sein. Die Details bezüglich Fallbearbeitung und Fallzuteilung werden im Rahmen der Dienstordnung sowie ausführender Weisungen geregelt.

c. Aus- und Weiterbildung

Um die Mitarbeitenden der Staatsanwaltschaft und der Jugendanwaltschaft im Allgemeinen mit Fachwissen im Bereich Cybercrime zu bedienen, wird der Fachbereich Cybercrime für die betriebsinterne Aus- und Weiterbildung zuständig sein. So soll er gewährleisten, dass sämtliche Mitarbeitende der Staatsanwaltschaft und der Jugendanwaltschaft in cybercrime-spezifischen Themen unterrichtet werden und stufengerecht die notwendigen Informationen erhalten, um die zugewiesenen Cybercrime-Fälle adäquat untersuchen zu können. Der Fachbereich soll hierfür die Kompetenz erhalten, Aus- und Weiterbildungsveranstaltungen selber oder allenfalls in Zusammenarbeit mit der Abteilung Cybercrime der Polizei durchzuführen bzw. zu organisieren.

d. Hotline

Der Fachbereich Cybercrime wird des Weiteren, wie erwähnt, eine Hotline zur Unterstützung der Staatsanwälte und Staatsanwältinnen und Untersuchungsbeauftragten der allgemeinen und besonderen Hauptabteilungen sowie der Jugendanwaltschaft betreiben. Dadurch soll bewerkstelligt werden, dass das Spezialwissen des Fachbereichs an alle Mitarbeitenden effizient weitergegeben werden kann und dass beispielsweise auch den Piketthabenden eine fachliche Unterstützung in Fällen von DigiKrim oder Cybercrime ieS zugesichert ist. Zudem soll die Hotline als Schnittstelle zur Polizei fungieren, über welche die Abteilung Cybercrime der Polizei den Fachbereich Cybercrime über neue Cybercrime-Fälle informieren oder mit dem Fachbereich Cybercrime sonstige cybercrime-bezogene Angelegenheiten besprechen kann.

Die Hotline soll in einem noch zu definierenden Turnus durch alle Mitglieder des Fachbereichs während der Bürozeiten betrieben werden.

2.8.2.4. Weitere Aufgaben und Zuständigkeiten des Fachbereichs Cybercrime

Neben der bereits erwähnten Hotline sollen die Mitarbeitenden des Fachbereichs zudem die Staatsanwälte und Staatsanwältinnen und Untersuchungsbeauftragten der allgemeinen und besonderen Hauptabteilungen im persönlichen Kontakt oder mittels fachlicher Besprechungen bei der Bearbeitung von Fällen digitalisierter Kriminalität, welche nicht durch den Fachbereich Cybercrime selbst bearbeitet werden, unterstützen.

Über die erwähnten Weiterbildungsveranstaltungen hinaus soll der Fachbereich Cybercrime die Mitarbeitenden der Staatsanwaltschaft zudem über die bestehenden internen Kanäle (Wissensplattform im Intranet [StawaWiki], INFOStawa, etc.) laufend über Aktualitäten im Bereich der Cyberkriminalität und deren Bekämpfung (neue Phänomene, «best practices», Mustervorlagen, etc.) informieren.

Schliesslich sollen dem Fachbereich Cybercrime noch die folgenden Aufgaben und Zuständigkeiten zukommen:

- Erarbeitung von Grundlagen für die Bearbeitung von Fällen DigiKrim und Cybercrime ieS, soweit erforderlich (Handbuch, Checklisten, Vorlagen, etc.)

- Betreibung und Pflege der Fachseite Cybercrime auf der Wissensplattform im Intranet (StawaWiki)

- Aufbereitung der benötigten statistischen Daten, Unterstützung bei der Erstellung von entsprechenden Statistiken respektive Bewirtschaftung der spezifischen Statistiken, insbesondere auch Lagebildern und Phänomene, soweit möglich und notwendig in Zusammenarbeit mit der Polizei Basel-Landschaft (Lage- und Informationszentrum)

- Zur-Verfügung-Stellen eines Tools, um Tatzusammenhänge bei Fällen von DigiKrim und Cybercrime ieS erkennen zu können (E-Mail-Konten, Bankkonten, IP-Adressen, etc.), soweit möglich und notwendig in Zusammenarbeit mit der Polizei Basel-Landschaft (Lage- und Informationszentrum)

- Pflege und Weiterentwicklung des kantonsinternen Cybercrime-Phänomenekatalogs sowie Abgleich und Anpassung an den nationalen Phänomenekatalog des fedpol

- Besetzung der Position des SPoC im nationalen Cyberboard (Mitarbeit in Cyber-CASE[15] und Cyber-STATE[16])

- Pflege von interkantonalem und internationalem Austausch im Bereich Cybercrime

- Einsitz oder Leitung in/von Arbeitsgruppen und Projekten im Bereich Cybercrime

[15] Cyber-CASE dient bei der operativen Bekämpfung von Cyberkriminalität als Schnittstelle zwischen den Staatsanwaltschaften der Kantone, der Bundesanwaltschaft sowie diversen mit der Thematik beschäftigten Stellen (MELANI, NEDIK, etc.). Es verfolgt insbesondere das Ziel, eine nationale Übersicht der aktuell pendenten Fälle zu generieren, diese Fallbearbeitung zu koordinieren, den Erfahrungs- und Wissensaustausch auf operativer Ebene sicherzustellen und spezifische operative Fragestellungen zu besprechen und Lösungen zu erarbeiten.

[16] Cyber-STATE verfolgt das Ziel, eine national konsolidierte Lagebildbeurteilung sicherzustellen, indem ein nationales Lagebild bezüglich Cyberkriminalitätsentwicklungen und Auswirkungen erstellt, Lageentwicklungsszenarien entwickelt und operative Handlungsempfehlungen abgeleitet werden. Alle im operativen Bereich des Cyberboards vertretenen Partner bringen selbständig lagerelevante Informationen ein und erstellen (wie bisher) ihr eigenes (Teil-)Lagebild.

2.8.2.5. Zusätzlicher personeller Ressourcenbedarf

Bisher stehen der Staatsanwaltschaft keine spezialisierten Staatsanwälte, Staatsanwältinnen und Untersuchungsbeauftragte für den Bereich Cybercrime ieS und DigiKrim zur Verfügung. Die anfallenden Fälle werden mit den zurzeit bestehenden personellen Ressourcen von sämtlichen Hauptabteilungen untersucht.

Basierend auf den erhobenen Fallzahlen, des erwarteten jährlichen Fallanstiegs um rund 20%, sowie angesichts der erwähnten Zusatzaufgaben, welche durch den Fachbereich Cybercrime zu bewältigen sein werden (Hotline, Weiterbildung, SPoC im Cyberboard, Prävention, Vernetzung allgemein, Leitung des Fachbereichs etc.), soll jener bei Betriebsaufnahme zunächst mit zwei Staatsanwälten oder Staatsanwältinnen und vier Untersuchungsbeauftragten besetzt sein. Da, wie ausgeführt, Fälle von Cybercrime ieS und komplexerer DigiKrim, die künftig dem Fachbereich Cybercrime zugeteilt werden sollen, bereits jetzt mit dem bestehenden Personalbestand untersucht werden, ist vorgesehen, den angestrebten Personalbestand vorerst zur Hälfte über interne Verschiebungen zu realisieren.

Ausgehend von 471 Anzeigen gemäss Statistik der Polizei für das Jahr 2018 und 224 Arbeitstagen pro Mitarbeitenden und Jahr[17], würden damit 235 Anzeigen auf jeden Staatsanwalt oder Staatsanwältin entfallen - also mehr als eine Anzeige pro Tag. Bei dieser Berechnung ist einerseits zu berücksichtigen, dass bei den erwähnten 471 Verfahren auch einige darunter sind, die später nicht durch den Fachbereich Cybercrime zu bearbeiten sind, weil sie nicht die nötige Komplexität aufweisen, oder auch solche, die mit einem geringeren Arbeitsaufwand zu erledigen sein werden. Andererseits ist jedoch zu beachten, dass Delikte im Bereich Cybercrime ieS oftmals sehr komplex und aufwändig zu untersuchen sind. Sie weisen internationale und interkantonale Bezüge auf und es sind meist zahlreiche Geschädigte vorhanden. So wurden beispielsweise in einem einzigen Zürcher Verfahren 2‘300 Geschädigte identifiziert. Schliesslich ist ganz allgemein auf Grund der zunehmenden Digitalisierung in allen Lebensbereichen auch von einer Zunahme der auszuwertenden Datenmengen und einer Zunahme von Bereichen, welche Gegenstand eines Cyberangriffes werden können, auszugehen (Stichwort Internet of Things).

Zudem wird ferner auch auf Grund der Tatsache, dass die Polizei mit ihrer neu gegründeten Abteilung Cybercrime mit im Endausbau 20 Mitarbeitenden gezielt einen Ermittlungsschwerpunkt im Bereich Cybercrime setzen und dadurch vermehrt entsprechende Verfahren generieren wird, mit einem Fallanstieg zu rechnen sein. Aktuell sind bei der Polizei lediglich zwei Ermittler im Nebenamt mit Cybercrime befasst, unterstützt durch eine massiv unterdotierte IT Forensik.

Nebst der eigentlichen Fallbearbeitung werden noch die vorstehend unter den Ziffern 2.8.2.3 und 2.8.2.4 aufgeführten Aufgaben und für den Leiter oder die Leiterin des Fachbereichs zusätzlich noch die damit zusammenhängenden Führungsaufgaben hinzukommen. Darüber hinaus muss sichergestellt werden, dass Ferien, krankheitsbedingte und sonstige Abwesenheiten aufgefangen werden können und dass jederzeit gewährleistet ist, dass ein Staatsanwalt oder eine Staatsanwältin verfügbar ist, der resp. die die erforderlichen Zwangsmassnahmen verfügen und die dringlichen Untersuchungshandlungen anordnen kann. Um den Betrieb des Fachbereichs Cybercrime, die zeit- und sachgerechte Bearbeitung der zugewiesenen Verfahren und insbesondere das Vorhandensein einer Ansprechperson in diesem Spezialgebiet jederzeit sicherzustellen, ist somit die bei der Staatsanwaltschaft angestrebte Stellenaufstockung um drei Stellen (zwei Staatsanwaltsstellen, eine Untersuchungsbeauftragtenstelle) unbedingt erforderlich.

Diesbezüglich sei des Weiteren auf den bereits erwähnten Revisionsbericht Nr. 024/2018 der Finanzkontrolle BL vom 11. September 2018 verwiesen, wonach mit dem vorhanden Personalbe-

[17] Anzahl Arbeitstage pro Jahr: 365 Tage abzüglich 52 Samstage, 52 Sonntage, 25 Ferientage, 9 gesetzliche Feiertage und 3 bezahlte arbeitsfreie Tage.

stand die bestehenden aktuellen Anforderungen nicht erfüllt werden können, weshalb empfohlen wird, die gemäss Projektstudie vorgeschlagenen Massnahmen, d.h. namentlich die hiermit beantragte Personalaufstockung zügig umzusetzen.

Mit den drei neu beantragten Stellen wird der Personalaufwand der Staatsanwaltschaft um rund CHF 416'000.00 zuzüglich 20% Sozialleistungen, somit total rund CHF 499'000.00 erhöht. Ein weiterer Ausbau des Fachbereichs Cybercrime ist aufgrund der Fallentwicklung sowie nach Vorliegen von ersten Erkenntnissen nach Inbetriebnahme durchaus möglich und denkbar und wird zu gegebener Zeit neu zu beurteilen sein.

2.9. Kosten für Raummieten und Mieterausbau (gemeinsam für Staatsanwaltschaft und Polizei)

In den aktuell vorhandenen Räumlichkeiten der Staatsanwaltschaft und der Polizei in der Gutsmatte können die 26 Arbeitsplätze und die weiteren erforderlichen Räumlichkeiten aus Platzgründen nicht untergebracht werden. Für die Umsetzung des Projektes Cybercrime kommt nur eine neue Einmietung in Frage. Eine passende freie Liegenschaft befindet sich zurzeit nicht im Portfolio des Kantons.

Ob und wie rasch eine passende Einmietung gefunden werden kann, ist zurzeit noch offen. Bei Anmietung von Räumen wird der erforderliche Mieterausbau je nach baulichem Aufwand und politischem Genehmigungsverfahren die entsprechende Zeit in Anspruch nehmen. Gemäss den erforderlichen Planungs-Genehmigungs- und Realisierungsprozessen werden die Räumlichkeiten für die neue Abteilung Cybercrime bis ca. 2022 zur Verfügung stehen. In der Anfangsphase muss der der Erstbedarf der Polizei und der Staatsanwaltschaft in bestehenden Räumen durch Auslagerungen und Verdichtungen abgedeckt werden.

Abschätzung Kosten für Raummiete und Mieterausbau:

Beim Raumbedarf geht das Hochbauamt von rund 1300 – 1600m^2 Geschossfläche aus. Rechnet man mit Mietkosten (core&shell) von rund CHF 250.00 m^2/a kommt man auf jährliche Kosten von CHF 400‘000.00. Hinzu kommt die Anmietung von 26 Parkplätzen mit jährlichen Kosten von CHF 43‘500.00.

Für die Abschätzung der Kosten für den Mieterausbau wurde als Referenzprojekt die Einmietung der Büroräumlichkeiten des Polizeistützpunkts im Schorenweg 10 in Arlesheim herangezogen (LRV 2011/194). Gemäss Abrechnung der LRV werden Ausbaukosten von CHF/m^2 1‘700.00 zuzüglich CHF/m^2 190.00 für Mobiliar und Umzüge ausgewiesen. Geht man von einem vergleichbaren Ausbaustandard aus, belaufen sich die geschätzten Kosten für den Mieterausbau auf ca. CHF 2‘210‘000.00-CHF 2‘720‘000.00 zuzüglich ca. CHF 247‘000.00 – CHF 304‘000.00 für Mobiliar und Umzüge.

Grobschätzung jährlich wiederkehrende Mietkosten (+/- 30 %):

Mietkosten (core&shell) für 26 Arbeitsplätze	
und Nebenräume (1300-1600 m^2) exkl. NK	CHF 299‘000.00 – 400‘000.00
Akonto Heiz- Nebenkosten, Reinigung (ca. 65 CHF/m2)	CHF 84'500.00 – 104'000.00
Mietkosten für 26 Parkplätze	CHF 43'500.00
Total wiederkehrende Kosten	**CHF 427’000.00 - 547'500.00**

Grobschätzung Kosten Mieterausbau (+/- 30 %)

Mieterausbau CHF 1700 x 1300-1600 m^2	CHF 2‘210‘000.00 – 2‘720‘000.00
Kosten für Mobiliar Ausstattung CHF 190/m^2	CHF 247‘000.00 – 304‘000.00
Total Mieterausbau und Mobiliar	**CHF 2‘457‘000.00 – 3‘024‘000.00**

Zum heutigen Zeitpunkt sind keine Kosten Für Mieten, Mieterausbau, Neben- und Betriebskosten budgetiert.

Da sich die Kosten für eine Einmietung gemäss Schätzung über CHF 200‘000.00 und rund CHF 3 Mio. für Mieterausbau belaufen, bedingen diese gemäss Finanzhaushaltsgesetz einen Landratsbeschluss. Mit Beschluss der Vorlage wird das Hochbauamt beauftragt, Lösungen für die Unterbringung der Arbeitsplätze zu evaluieren und die terminliche Umsetzbarkeit abzuklären, erforderlichen Kosten ins Budget aufzunehmen und die entsprechenden Ausgabenbewilligungen zu beantragen.

2.10. Risiken bei Nichtumsetzung der Strategie Cybercrime

Kann die Strategie Cybercrime nicht umgesetzt werden, könnte das für die Bekämpfung der Cyberkriminalität notwenige Know-How nicht in genügendem Umfang aufgebaut werden. Die Mittel für eine erfolgreiche Zusammenarbeit zwischen Polizei und Staatsanwaltschaft wären nicht vorhanden und die Aufgaben der Strafverfolgung könnten nicht ausreichend wahrgenommen werden. Dies hätte zur Folge, dass Delikte im Cyberbereich nicht in der geforderten Qualität und Quantität bearbeitet und verfolgt werden könnten. So würden beispielsweise die Bearbeitungsfristen bei der IT-Forensik auch künftig (zu) lange dauern und es bestünde die Gefahr, dass bei etlichen Verfahren das Beschleunigungsgebot verletzt und damit eine Reduktion des Strafmasses drohen würde. Die mangelhaften Möglichkeiten der Strafverfolgung würden die Entstehung eines rechtsfreien Raumes begünstigen. Die Aufklärungsquoten würden tief bleiben und die Kriminalität im Cyberbereich würde sich sehr schnell und unkontrolliert weiterentwickeln. Aufgrund der fortschreitenden Digitalisierung der Gesellschaft wäre davon ein sehr grosser Teil der Bevölkerung betroffen. Das Vertrauen der Bevölkerung in die Institutionen der Strafverfolgung würde leiden und es würde ein Reputationsschaden drohen.

2.11. Strategische Verankerung / Verhältnis zum Regierungsprogramm

Im Regierungsprogramm des Kantons Basel-Landschaft 2016 bis 2019 bildet die Umsetzung der neuen Sicherheitsstrategie einen Schwerpunkt, namentlich mit dem Ziel, den Kanton Basel-Landschaft zu einem der sichersten Kantone der Schweiz zu machen. Präventive und repressive Massnahmen sollen namentlich den Schutz vor Kriminalität verstärken, wobei neue Erscheinungsformen der Kriminalität – wie beispielsweise im Bereich Cybertechnik – besonders zu beachten sind. Das entsprechende Legislaturziel ZL-LZ 5 (ZL-RZD 14), das sich u.a. an Polizei und Staatsanwaltschaft richtet, sieht konkret vor, dass sich der Kanton zum Ziel setzt, «dass Baselland ge-

messen an der Zahl der Straftaten […] zu den sichersten Kantonen gehört (mit Werten deutlich unter dem schweizerischen Mittelwert)». Dazu ist u.a. die Cyberkriminalität, d.h. «die Begehung von Straftaten durch missbräuchlichen Gebrauch elektronischer Kommunikationsmittel», zu verhindern und zu bekämpfen.
Gemäss Aufgaben- und Finanzplan 2018 bis 2021 (Beschluss Landrat, LRV 2017/250, LRB 2017/1827) ergeht u.a. der Leistungsauftrag an die Sicherheitsdirektion, der Cyberkriminalität wirksam entgegenzutreten. Im Besonderen soll die Polizei Basel-Landschaft im Bereich «Cybercrime» Grundwissen an die Frontmitarbeitenden vermitteln und im Rahmen ihrer Ressourcen den Bereich «Cybercrime», im Einklang mit der gesamtschweizerischen Ausrichtung, weiter aufbauen. Da die Entwicklung im Bereich Technik und Taktik schnell voranschreitet und die «Gegenseite» diese Entwicklungen nutzt, soll «die gesamtschweizerische Zusammenarbeit im Bereich Polizeitechnik und -informatik für qualitativ sehr gute und kostengünstige Lösungen genutzt werden».

2.12. Rechtsgrundlagen und Finanzreferendum

2.12.1. Rechtsgrundlagen

- Strafgesetzbuch (StGB, SR 311.0)
- Strafprozessordnung (StPO, SR 312.0)
- Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO, SGS 250)
- Dekret zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (Dekret EG StPO, SGS 250.1)
- Polizeigesetz des Kantons Basel-Landschaft (PolG, SGS 700)

2.12.2. Finanzreferendum

Aufgrund der Höhe der zu bewilligenden Ausgabe (vgl. Beschluss) untersteht der Beschluss des Landrates in Bezug auf die Ausgabenbewilligung der fakultativen Abstimmung gemäss § 31 Abs. 1 Buchstabe b der Kantonsverfassung.

2.13. Finanzielle Auswirkungen

Rechtsgrundlage und rechtliche Qualifikation (§ 35 Abs. 1 Bst. a–b Vo FHG):

Vgl. Ziff.2.12.1 (§ 33 Abs. 2 FHG)							
Die Ausgabe ist …(§ 34 und § 35 FHG)							
X	Neu		Gebunden		Einmalig	X	Wiederkehrend

Ausgabe (§ 35 Abs. 1 Bst. b–f Vo FHG):

Budgetkredit:	Profit-Center: 2420 Profit-Center Stawa: 2450		Kt: 30	Diverse Konten	Kontierungsobj.:	Diverse
Verbuchung	X	Erfolgsrechnung		Investitionsrechnung		

Erfolgsrechnung ☒ Ja ☐ Nein

	Voraussichtlich jährlich anfallende Beträge:	PC	Kt	2020	2021	2022	2023	2024	2025
A	Personalkosten Polizei 1)	2420	30	533'876	1'127'049	1'364'321	1'601'589	1'601'589	1'601'589
A	Personalkosten Stawa	2450	30	499'000	499'000	499'000	499'000	499'000	499'000
A	Sach- und Betriebsaufw.		31						
A	Transferaufwand		36	0	0	0	0	0	0
A	Bruttoausgabe			1'032'876	1'626'049	1'863'321	2'100'589	2'100'589	2'100'589
E	Beiträge Dritter*		6	0	0	0	0	0	0
	Nettoausgabe			1'032'876	1'626'049	1'863'321	2'100'589	2'100'589	2'100'589

* Gemäss § 36 Abs. 3 FHG; PC = Profitcenter; Kt = Kontengruppe
1) Der Aufbau der Abteilung Cybercrime erfolgt schrittweise (siehe auch Kapitel 2.8)

Auswirkungen auf den Aufgaben- und Finanzplan (§ 35 Abs. 1 Bst. j Vo FHG):

Die Kosten werden in den Aufgaben- und Finanzplan eingepflegt.

Weitere Einnahmen (§ 35 Abs. 1 Bst. f Vo FHG):

Keine

Folgekosten (§ 35 Abs. 1 Bst. g Vo FHG):

	Zusammenfassung Folgekosten in CHF		PC	Kt	2020	2021	2022	2023
A	1	**Nettoinvestitionen**						
A	2	Zusätzliche Betriebskosten IT SID wiederkehrend (IT-Mittel)	**24004**	**31**	171'500	109'000	108'000	120'000
A	2	Zusätzliche Betriebskosten IT SID einmalig (Datenleitungen, Server)	**24004**	**31**		118'500		
		Zusätzliche Betriebskosten HBA wiederkehrend (Miete) (siehe Kapitel 2.9)	**2304**	**31**	547'500	547'500	547'500	547'500
		Zusätzliche Betriebskosten HBA einmalig (Ausbau)	**2304**	**31**		3'024'000		
		Zusätzliche Betriebskosten TBA wiederkehrend (Fahrzeuge)	**2302**	**31**	130'000	115'500		
A		Abschreibungen		**33**	**0**	**0**	**0**	**0**
A		Zinskosten *Kalk. Zinssatz* ***1.168 %***		**34**	**0**	**0**	**0**	**0**
A		**Folgekosten brutto**			**849'000**	**3'914'500**	**656'000**	**667'500**
A	3	**Folgeertrag brutto**		**42/43**	**0**	**0**	**0**	**0**
E	2-3	**Folgekosten netto**			**849'000**	**3'914'500**	**656'000**	**667'500**
A	**Rückbaukosten:**							
	4	**Zusätzliche Stellenprozent in FTE Polizei**			**4**	**7**	**11**	**13**
	4	**Zusätzliche Stellenprozent in FTE Stawa**			**3**	**3**	**3**	**3**

PC = Profitcenter; Kt = Kontengruppe

Auswirkungen auf den Stellenplan (§ 35 Abs. 1 Bst. i Vo FHG):

Der Stellenplan muss um die beantragten unbefristeten Stellen erhöht werden.

Die Umsetzung der Strategie «Cybercrime» gemäss dieser Landratsvorlage kann möglicherweise zu einer Mehrbelastung der Gerichte führen, die zu einer Anpassung der personellen Ressourcen führen kann. Eine konkrete Einschätzung, in welchem Rahmen diese Anpassung erfolgen wird, kann zum heutigen Zeitpunkt aufgrund fehlender Erfahrungswerte nicht gemacht werden.

Schätzung der Eigenleistungen (§ 35 Abs. 1 Bst. h Vo FHG):

Keine

Strategiebezug (§ 35 Abs. 1 Bst. m Vo FHG):

[EESH-RZD 1]	Vgl. Ziff. 2.4.

Risiken (Chancen und Gefahren) (§ 35 Abs. 1 Bst. l Vo FHG):

Chancen	Gefahren
Stärkung der Kompetenzen der Strafverfolgungsbehörden im Bereich der Bekämpfung von Cybercrime	Trotz neu geschaffener Stellen verbessert sich die Aufklärungsquote nicht wesentlich. Trotz hohem finanziellem Aufwand bleibt der Erfolg bescheiden.
Stärkung des Sicherheitsgefühls der Bevölkerung	Rekrutierung von Personen mit entsprechender Ausbildung kann ev. schwierig sein, da die speziell ausgebildeten Personen nicht angemessen entlöhnt werden können.
Gewährleistung der Rechtssicherheit im Cyberraum (kein rechtsfreier Raum)	Obwohl die Kompetenzen der Strafverfolgungsbehörden bei der Verfolgung von Delikten im Bereich Cybercrime erhöht wird, kann insbes. die international tätige Täterschaft nicht an erneuter Delinquenz gehindert werden
Beitrag zur Gewährleistung der Rechtssicherheit des Wirtschaftsstandortes Baselland	
Gewährleistung / Steigerung der Reputation der Institutionen des Kantons Basel-Landschaft	

Zeitpunkt der Inbetriebnahme (§ 35 Abs. 1 Bst. n Vo FHG):

Januar 2020

Wirtschaftlichkeitsrechnung (§ 35 Abs. 1 Bst. k, § 49–51 Vo FHG):

Mit der Umsetzung der Strategie Cybercrime werden die Staatsanwaltschaft und die Polizei Basel-Landschaft befähigt und mit Mitteln ausgestattet, die es ihnen ermöglichen, Delikte im Bereich Cybercrime wirkungsvoll und zielgerichtet zu bekämpfen.

Im Bereich der Prävention erlaubt die Strategie Cybercrime der Polizei Basel- Landschaft, potentiell Betroffene gezielt anzusprechen und zu sensibilisieren. Mit einer wirkungsvollen Prävention können Delikte verhindert und Schäden vermieden werden.

Die koordinierte und kontinuierliche Aus- und Weiterbildung der Mitarbeitenden der Polizei sowie der Staatsanwaltschaft bewirken, dass das erforderliche Wissen vorhanden ist, um die Cybercrime Delikte überhaupt nachhaltig bekämpfen zu können. Ohne eine gezielte Aus- und Weiterbildung ist dies nicht möglich. Ebenfalls unabdingbar für eine Bekämpfung von Cybercrime- Delikten ist die enge Zusammenarbeit zwischen den Strafverfolgungsbehörden. Mit der Strategie, die die Organisation der Zusammenarbeit ins Zentrum stellt, wird eine Strafverfolgung in diesem Bereich erst ermöglicht.

Der Aufbau der vorerwähnten Fähigkeiten trägt massgebend zu einem sicheren Wirtschaftsstandort Baselland bei.

Andere Optionen, die eine wirkungsvolle Bekämpfung von Cybercrime Delikten ermöglichen, bestehen aktuell nicht.

2.14. Finanzrechtliche Prüfung

Die Finanz- und Kirchendirektion hat die Vorlage gemäss § 12 des Finanzhaushaltsgesetzes geprüft und stellt fest, dass die Grundsätze der Haushaltsführung und die Kompetenzordnung eingehalten sind.

2.15. Regulierungsfolgenabschätzung

Mit der Umsetzung der Strategie zur Bekämpfung der Cyberkriminalität entstehen für die Gemeinden und die Unternehmen im Kanton Basel-Landschaft keine zusätzlichen finanziellen oder administrativen Belastungen. Die Umsetzung der Strategie hat ausschliesslich finanzielle und organisatorische Auswirkungen auf den Kanton.

2.16. Vorstösse des Landrates

Mit dieser Vorlage wird das Postulat 2017/186: «Kantonale Strategie Cyber-Kriminalität» beantwortet.

3. Anträge

3.1. Beschluss

Der Regierungsrat beantragt dem Landrat zu beschliessen:

1. Von der Strategie der Polizei Basel-Landschaft und der Staatsanwaltschaft zur Bekämpfung der Cyberkriminalität wird zustimmend Kenntnis genommen.

2. Für die Umsetzung der unter Ziff. 1 erwähnten Strategie zur Bekämpfung der Cyberkriminalität wird ab 2020 eine neue wiederkehrende Ausgabe von CHF 2'100’589.00 pro Jahr bewilligt.

3. Von den einmaligen Folgekosten im Betrag von CHF 3'142'500.00 wird Kenntnis genommen.

4. Von den wiederkehrenden Folgekosten im Betrag von CHF 849'000.00 pro Jahr wird Kenntnis genommen.

5. Das Hochbauamt wird beauftragt, Lösungen für die Unterbringung der Arbeitsplätze zu evaluieren, die erforderlichen Kosten ins Budget aufzunehmen und die entsprechenden Ausgabenbewilligungen zu beantragen.

6. Das Dekret zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (SGS 250.1) wird gemäss Beilage geändert.

7. Ziffer 2 des vorliegenden Landratsbeschlusses untersteht gemäss § 31 Absatz 1 Buchstabe b der Kantonsverfassung der fakultativen Volksabstimmung.

3.2. Abschreibung von Vorstössen des Landrates

Der Regierungsrat beantragt dem Landrat die Abschreibung des folgenden Vorstosses mit entsprechender Begründung:

1. Postulat: 2017/186: «Kantonale Strategie Cyber-Kriminalität»

Liestal, 25. Juni 2019

Im Namen des Regierungsrats

Die Präsidentin:

Monica Gschwind

Die Landschreiberin:

Elisabeth Heer Dietrich

4. Anhang

– Entwurf Landratsbeschluss
– Entwurf Dekretsänderung
– Entwurf Synopse

Landratsbeschluss

über Projekt Cybercrime (Ausgabenbewilligung; Änderung des Dekrets zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (Dekret EG StPO); Beantwortung Postulat 2017/186 «Kantonale Strategie Cyber-Kriminalität»)

Der Landrat des Kantons Basel-Landschaft beschliesst:

1. Von der Strategie der Polizei Basel-Landschaft und der Staatsanwaltschaft zur Bekämpfung der Cyberkriminalität wird zustimmend Kenntnis genommen.

2. Für die Umsetzung der unter Ziff. 1 erwähnten Strategie zur Bekämpfung der Cyberkriminalität wird ab 2020 eine neue wiederkehrende Ausgabe von CHF 2'100’589.00 pro Jahr bewilligt.

3. Von den einmaligen Folgekosten im Betrag von CHF 3'142'500.00 wird Kenntnis genommen.

4. Von den wiederkehrenden Folgekosten im Betrag von CHF 849'000.00 pro Jahr wird Kenntnis genommen.

5. Das Hochbauamt wird beauftragt, Lösungen für die Unterbringung der Arbeitsplätze zu evaluieren, die erforderlichen Kosten ins Budget aufzunehmen und die entsprechenden Ausgabenbewilligungen zu beantragen.

6. Das Dekret zum Einführungsgesetz zur Schweizerischen Strafprozessordnung (SGS 250.1) wird gemäss Beilage geändert.

7. Ziffer 2 des vorliegenden Landratsbeschlusses untersteht gemäss § 31 Absatz 1 Buchstabe b der Kantonsverfassung der fakultativen Volksabstimmung.

8. Das Postulat 2017/186 «Kantonale Strategie Cyber-Kriminalität» wird infolge der Beantwortung im Sinne von Ziff. 1 und 2 des Beschlusses als erfüllt abgeschrieben.

Liestal, Datum wird von der LKA eingesetzt!

Im Namen des Landrates

Der Präsident:

Die Landschreiberin: